Digitaaliset identiteettivarkaudet ja rahanpesu: Turvallisuus finanssialalla

Suvi Sutinen

2024 Laurea

Laurea-ammattikorkeakoulu

Digitaaliset identiteettivarkaudet ja rahanpesu: Turvallisuus finanssialalla

Suvi Sutinen
Liiketalouden koulutus
Opinnäytetyö
Toukokuu, 2024

Laurea-ammattikorkeakoulu **Tiivistelmä**

Liiketalouden koulutusohjelma

Tradenomi (AMK)

Suvi Sutinen

Digitaaliset identiteettivarkaudet ja rahanpesu: Turvallisuus finanssialalla

Vuosi 2024 Sivumäärä 58

Tämän opinnäytetyön tavoitteena oli tutkia lainopillisesta näkökulmasta digitaalisia identiteettivarkauksia ja rahanpesua sekä näiden vaikutusta turvallisuuteen finanssialalla. Tarkoituksena oli selvittää, miten digitaaliset identiteettivarkaudet esiintyvät, mikä niiden asema on osana suomalaista lainsäädäntöä, tarkastella identiteettivarkauksia ilmiönä sekä osana petosrikollisuutta. Lisäksi tarkasteltiin rahanpesun asemaa osana suomalaista lainsäädäntöä sekä tutkittiin rahanpesua ilmiönä painottaen sen asemaa kotimaisessa kontekstissa. Keskiössä on myös ilmiöiden yleisyys Suomessa ja niitä tutkittiin myös finanssialan turvallisuuden näkökulmasta. Tavoitteena oli selvittää, millaisia riskejä digitaaliset identiteettivarkaudet ja rahanpesu tuovat mukanaan pankkijärjestelmälle sekä kartoittaa erilaisia strategioita finanssialan turvallisuuden parantamiseksi näiltä osin. Opinnäytetyö tarjoaa tietoa käsiteltävien aiheiden lainsäädännöstä, ilmiöiden yleisyydestä, niiden erikoispiirteistä ja vaikutuksista finanssialan turvallisuuteen sekä erilaisista keinoista parantaa finanssialan turvallisuutta teknologian avulla.

Teknologian ja rahoitusteknologian, eli FinTechin nopea kehitys ja kasvava petosrikollisuuden määrä luo kasvavia tarpeita finanssialan turvallisuuden toteuttamiseksi. Turvallisuus finanssialalla lainsäädännöllisestä näkökulmasta perustuu vahvasti Euroopan unionin sääntelyyn, kansainvälisiin sopimuksiin ja suosituksiin. Opinnäytetyön painotus nojaa vahvasti nykyteknologian luomiin mahdollisuuksiin toteuttaa petos- sekä rahanpesurikollisuutta mutta samaten myös mahdollisuuksiin ennaltaehkäistä ja estää näitä rikoksia. Työssä tarkastellaan myös lainsäädännön asemaa rikollisuuden ennaltaehkäisyn ja selvittämisen keinona. Teoreettinen viitekehys perustuu vahvasti Euroopan unionin lainsäädäntöön sekä kansalliseen lainsäädäntöön, lain esitöihin sekä asiantuntijoiden tuottamaan tietoon.

Aiheita lähestyttiin oikeusdogmaattisesta eli lainopillisesta sekä empiirisestä näkökulmasta, jolloin työssä on voitu tarkastella valittuja aiheita lain soveltamisen ja tulkitsemisen kannalta. Oikeusdogmaattinen lähestymistapa aiheeseen on siten mahdollistanut lain tulkitsemisen huomioiden sen yksityiskohdat, lainsäädännön taustat ja tarkoitukset, lainsäädäntöprosessin, lainsäädännön muutosten ja uudistusten tarpeellisuuden sekä niiden vaikutuksen käytännön tasolla. Lisäksi empiirinen lähestymistapa lisää ymmärrystä opinnäytetyön aiheista osana yhteiskunnallisia ilmiöitä korostaen niiden vaikutusta kansalaisiin.

Tuloksissa ilmeni petosrikollisuuden määrän voimakas kasvu ja sen yhteys kansainväliseen rikollisuuteen. Valtaosa petoksista tapahtuu tietoverkkoavusteisesti ja korruptiolla oli yhteys rahanpesuun ja järjestäytyneeseen rikollisuuteen EU:n alueella. Tyypillisimpiä rahanpesun esirikoksia Suomessa olivat petosrikokset. Myös teknologian kehityksellä oli yhteyttä rikollisuuden kehittyneisyyteen, ja tämä havaittiin myös finanssialan turvallisuusriskinä. Opinnäytetyö tarjoaa katsauksen lainsäädännöllisiin näkökulmiin ja esittää keinoja finanssialan turvallisuuden yksityiskohtien huomioimiseksi ottaen huomioon teknologian kehityksen. Opinnäytetyö pyrkii toimimaan tiedonlähteenä niin kansalaisille kuin finanssialan toimijoillekin lisäten tietoa ja ymmärrystä digitaalisten identiteettivarkauksien ja rahanpesun mekanismeista, riskeistä ja käytännöistä turvallisuuden parantamiseksi finanssialalla. Tiedon tuottaminen ja lisääminen erilaisista verkon kautta tapahtuvista hyökkäyksistä ja rikoksista sekä niiden estämisestä on merkittävää myös yhteiskunnallisesti.

Asiasanat: identiteettivarkaus, rahanpesu, turvallisuus, finanssiala, lainsäädäntö

Laurea University of Applied Sciences

Degree Program of Business Administration

Bachelor of Business Administration

Suvi Sutinen

Abstract

Digital identity theft and money laundering: Security in the financial sector

Year 2024 Pages 58

The aim of this thesis was to examine digital identity theft and money laundering from a legal perspective and their impact on the security of the financial sector. The objective was to investigate how digital identity theft happens, its legal status within Finnish legislation, and to examine identity theft both as a phenomenon and as part of fraud crime. Additionally, the position of money laundering in Finnish legislation was examined, emphasizing its role in the domestic context. The focus was also on the prevalence of digital identity theft and money laundering in Finland, with a consideration of these topics from the perspective of financial sector security. The goal was to identify the risks that digital identity theft and money laundering pose to the banking system and to present strategies to enhance financial sector safety in these areas. The thesis provides insights into the legislation, prevalence, characteristics, and effects of digital identity theft and money laundering on financial sector security, as well as methods to improve security through technology.

The rapid development of technology and financial technology (FinTech), along with the increasing number of fraudulent activities, creates growing demands for ensuring security in the financial sector. Security in the financial sector from a legislative standpoint heavily relies on European Union regulations, international agreements, and recommendations. The emphasis of this thesis is strongly placed on the opportunities created by current technology to carry out and prevent fraud and money laundering crimes. This thesis also examines the role of legislation in preventing and investigating criminal activities. The theoretical framework of the thesis is heavily based on European Union and national legislation, legislative preparations, and expert knowledge.

The topics were approached from a legal and empirical perspective, allowing for an examination of selected topics from the standpoint of law application and interpretation. This approach enabled a detailed understanding of the law, its background, legislative processes, and the need for changes and reforms. The empirical perspective highlighted the societal impact of these topics.

The results revealed a significant increase in fraud crimes and their connection to international crime. Most frauds occur online, and corruption was linked to money laundering and organized crime in the EU. In Finland, fraud crimes were the most common predicate offenses for money laundering. The development of technology was also linked to the sophistication of criminal activities, which was noted as a security risk for the financial sector. This thesis provides an overview of legislative perspectives and suggests ways to enhance financial sector security by considering technological advancements. It aims to be a source of information for both citizens and financial sector operators, increasing knowledge and understanding of the mechanisms, risks, and practices related to digital identity theft and money laundering to improve security in the financial sector. Producing information about online attacks and crimes and their prevention is also important from a societal perspective.

Keywords: identity theft, money laundering, security, financial sector, legislation

Sisällys

1 Johdanto

Tässä opinnäytetyössä tavoitteena oli tarkastella digitaalista identiteettivarkautta ja rahanpesua lainopillisesta näkökulmasta sekä niiden vaikutusta finanssialan turvallisuuteen. Tutkimuksessa keskityttiin selvittämään digitaalisen identiteettivarkauden ilmenemistä, sen asemaa suomalaisessa lainsäädännössä ja sen roolia petosrikollisuudessa. Lisäksi tutkittiin rahanpesun asemaa osana suomalaista lainsäädäntöä sekä sen merkitystä kotimaisessa kontekstissa. Opinnäytetyössä arvioitiin myös digitaalisten identiteettivarkauksien ja rahanpesun yleisyyttä Suomessa sekä niiden vaikutuksia finanssialan turvallisuuteen, samalla tarkastellen erilaisia strategioita turvallisuuden parantamiseksi finanssialalla. Lisäksi työssä käydään läpi käytännön tapausesimerkkejä rahanpesun ja identiteettivarkauksien ilmentymisestä, jotta aiheesta saatava käsitys olisi mahdollisimman kattava.

Aihe on ajankohtainen, sillä petosrikollisuuden määrä on voimakkaassa kasvussa ja yhä useampi jokapäiväinen toiminta hoidetaan verkossa.[1] Esimerkiksi suomalaiseen poliisihallintoon perustetaan tietoverkkoavusteisiin petoksiin keskittyvä tutkimusyksikkö, jotta suurten petoskokonaisuuksien selvittäminen olisi tehokkaampaa. Petosrikollisuus on muuttunut organisoidumpaan ja järjestäytyneempään muotoon, ja sen taustalla onkin usein järjestäytynyttä rikollisuutta ja jopa rahanpesua. Suurin osa petosrikollisuudesta tapahtuu tietoverkkoavusteisesti ja EU:n alueella eri petosten tuottama taloudellinen hyöty on miljardeja euroja vuosittain.[2] Identiteettivarkaudet ovat ylivoimaisesti yleisin petoksen muoto Suomessa, ja ne kytkeytyvät usein muihin petosrikoksiin.[3] Lisäksi teknologian ja rahoitusteknologian nopea kehitys ovat luoneet pohjan kyberrikollisuuden ja petosten toteuttamiselle sekä kehittymiselle. Rikollisten teknologiset harppaukset etenevät sitä mukaa, kun uutta teknologiaa ja muita innovaatioita syntyy.[4]

Tämä luo kasvavan tarpeen tarkastella finanssialan turvallisuuteen liittyviä seikkoja ja strategioita tarkemmin. Tiedon tuottaminen ja lisääminen erilaisista verkon kautta tapahtuvista hyökkäyksistä ja näihin liittyvistä rikoksista sekä niiden estämisestä on merkittävää yhteiskunnallisesti niin kansalaisten kuin julkisten ja yksityistenkin toimijoiden kannalta. Opinnäytetyön yhtenä tavoitteena on lisätä tietoa ja ymmärrystä digitaalisten identiteettivarkauksien ja rahanpesun mekanismeista ja riskeistä, sillä keskiössä petosrikollisuuden ehkäisyssä on myös kansalaisten oma aktiivisuus ja tarkkaavaisuus näiden aiheiden suhteen. Teknologian nopea

[1] Tanttari & Alanko 2017, 12; Hasham, Joshi & Mikkelsen 2019, 2; Kyberturvallisuuskeskus 2023, 1.
[2] OECD 2006, 4; Rahanpesun selvittelykeskus 2023, 2 & 35; Europol 2024a, 4–5.
[3] Näsi & Tanskanen 2017, 158; Näsi 2022, 134.
[4] Savona & Manzoni 2013, 2; Hasham, Joshi & Mikkelsen 2019, 2; KPMG 2023, 1.

kehitys on vaatinut lainsäädännön päivittämistä ja uudistamista, ja tässä työssä tarkastellaan myös lainsäädännön asemaa rikollisuuden ennaltaehkäisyn ja selvittämisen keinona.

Keskeisenä lähdeaineistona on hyödynnetty Suomen rikoslakia (39/1889), lain esitöitä, oikeuskäytäntöä, oikeuskirjallisuutta -ja tutkimusta, artikkeleita ja muuta asiantuntijoiden ja viranomaisten tuottamaa tietoa. Opinnäytetyö lähtee liikkeelle sen tavoitteen ja tutkimusmenetelmien määrittelystä ja tarkastelusta. Opinnäytetyön tutkimusmenetelmäksi on valittu oikeusdogmaattinen eli lainopillinen lähestymistapa, jolloin työssä on voitu tarkastella valittuja aiheita lain soveltamisen ja tulkitsemisen kannalta ja voitu lisätä ymmärrystä opinnäytetyön aiheista oikeudellisesta näkökulmasta ja siten myös korostaa oikeudellisen tiedon merkitystä. Lisäksi opinnäytetyön aiheita lähestytään lainopin ulkopuolisesta, eli empiirisestä näkökulmasta, jotta aiheista saatava kokonaiskuva olisi tarpeeksi kattava.

Opinnäytetyö etenee tarkastelemaan identiteettivarkauksia ilmiönä sekä sen asemaa osana suomalaista lainsäädäntöä. Työssä käydään läpi identiteettivarkauden mekanismeja, eli toteuttamismuotoja ja niiden erityispiirteitä sekä tutkitaan identiteettivarkauksien asemaa osana muuta rikollisuutta. Lisäksi työssä sivutaan myös muita kyberrikoksia ja petoksia, niiden yleisyyttä sekä niiden asemaa suomalaisessa lainsäädännössä. Tämän jälkeen opinnäytetyössä siirrytään käsittelemään rahanpesua ilmiönä, sen asemaa osana suomalaista lainsäädäntöä sekä rahanpesun toteuttamismuotoja. Työssä tutkitaan rahanpesun yleisyyttä ja sen asemaa osana muuta talousrikollisuutta. Viimeisimpänä opinnäytetyössä tutkitaan finanssialan turvallisuutta ottaen huomioon rahoitusalan toimijoiden kohtaamat turvallisuusriskit aiemmin käsiteltyjen rikollisuuden teemojen pohjalta sekä käytänteet näihin riskeihin vastaamiseksi. Lisäksi opinnäytetyössä käydään läpi teknologian luomia mahdollisuuksia finanssialan tulevaisuudelle ja turvallisuudelle sekä esitellään erilaisia malleja turvallisuuden parantamiseksi osana organisaatioiden strategiaa. Viimeisessä käsittelykappaleessa käydään läpi identiteettivarkauksien sekä rahanpesun ilmenemismuotoja yhtenäisenä kokonaisuutena aiheen monimuotoisuuden käsittämiseksi. Lopuksi työssä käydään läpi yhteenveto opinnäytetyöstä ja eritellään työn pohjalta syntyneitä johtopäätöksiä.

2 Opinnäytetyön tavoite ja tutkimusmenetelmä

Tämän opinnäytetyön päämääränä oli syventyä digitaalisen identiteettivarkauden ja rahanpesun lainopillisiin näkökulmiin ja niiden vaikutuksiin liittyen finanssialan turvallisuuteen. Tavoitteena oli analysoida digitaalisten identiteettivarkauksien esiintymistä, niiden asemaa Suomen lainsäädännössä ja niiden roolia osana petosrikollisuutta. Lisäksi tutkittiin rahanpesun merkitystä suomalaisessa lainsäädännössä ja sen ilmenemistä kotimaisessa kontekstissa. Tutkimuksessa keskityttiin myös digitaalisten identiteettivarkauksien ja rahanpesun yleisyyteen Suomessa sekä niiden vaikutukseen finanssialan turvallisuuden kontekstissa. Tavoitteena oli

tunnistaa digitaalisten identiteettivarkauksien ja rahanpesun aiheuttamat riskit pankkijärjestelmälle ja asiakkaille sekä esitellä erilaisia strategioita finanssialan turvallisuuden tehostamiseksi. Opinnäytetyö tarjoaa tietoa näiden aiheiden lainsäädännöstä, esiintymisestä ja yleisyydestä, erityispiirteistä ja aiheiden vaikutuksista finanssialan turvallisuuteen sekä keinoista alan turvallisuuden parantamiseksi.

Opinnäytetyössä käsiteltäviä aiheita lähestytään lainopillisesta, eli oikeusdogmaattisesta näkökulmasta. Lainopin tutkimuksessa keskitytään voimassa olevaan, eli velvoittavaan oikeuteen, ja sen avulla tutkitaan voimassa olevien oikeusnormien[5] sisältöä. Lainopin metodit perustuvat tulkintaan, sillä se on merkitykseltään oikeudellisten tekstien tulkintaa, oikeusjärjestyksen[6] sääntöjen tarkastelemista sekä niiden merkityksen ja sisällön tutkimista. Yleensäkin oikeustiedettä lähellä olevat tieteenalat ovat teologia, kirjallisuustiede ja toisaalta myös kielitiede, sillä myös niissä keskeistä on tekstien tulkinta ja sanojen sekä tekstin merkitykset, eli semantiikka tai merkitysoppi.[7] Voimassa olevan oikeuden sisältö liittyen käsiteltävään aiheeseen tai oikeusongelmaan on lainopin tyypillisin tutkimusongelma, eli toisin sanoen lainopin avulla pyritään saamaan vastaus siihen, kuinka todellisessa tilanteessa tulisi toimia oikeusjärjestyksen, eli velvoittavan oikeuden, mukaan. Lainopin toisena tehtävänä on oikeusjärjestyksen jäsentäminen, eli systematisointi. Systematisoinnin avulla pyritään selkeyttämään säännösten löydettävyyttä, rakentamaan oikeudellisten käsitteiden systeemiä sekä havaitsemaan keskinäisien oikeudellisien suhteiden yleiskuvaa.[8] Oikeustieteellisen tutkimuksen metodit ovat usein hajanaisia mutta monimuotoisia, ja eri metodien avoimuus ja joustava käyttö on yleistä oikeudellisissa tutkimuksissa.[9]

Toisaalta opinnäytetyössä hyödynnetään menetelmänä myös empiiristä suuntausta, jossa otetaan huomioon lainopin ulkopuolelle jäävät seikat. Esimerkiksi Yhdysvalloissa 1800–1900 luvun taitteessa oikeustieteisiin alettiin yhdistämään empiiriseen tutkimukseen pohjautuen oikeudellista realismia, joka rakentui sosiologisesta ja psykologisesta teorianmuodostuksesta. Suuntauksessa keskeistä oli oikeuden tosiasiallinen soveltaminen sekä yhteiskunnassa todellisuudessa vaikuttavan oikeuden ja kirjaoppineiden oikeuden erottaminen toisistaan. Oikeusrealismin suuntauksen tarkoituksena oli oikeudellisen päätöksenteon ohjaaminen ja irrallisten seikkojen karsiminen. Yhteisenä ajatuksena oli, että myös juridiikan ulkopuolelle jäävillä seikoilla

---

[5] Ks. Hirvonen 2011, 23–24. Ks. myös Eduskunta 2024. Oikeusnormien tehtävänä on säännellä tekemistä esimerkiksi sallien tai kieltäen jotakin. Oikeusnormi sisältää siis sekä oikeusnormilauseen ja oikeusnormin ajatussisällön. Oikeusnormilause tuottaa tietoa oikeusnormista, esimerkiksi kieltämällä jonkun toiminnan tietyssä kontekstissa, ja oikeusnormin ajatussisältö koostuu tulkitusta merkityksestä. Oikeusnormi voi siis olla esimerkiksi lakipykälä.
[6] Ks. Tuori 2013, 14. Oikeusjärjestys on oikeusnormien muodostama joukko, eli velvoittava oikeus.
[7] Hirvonen 2011, 21–22 & 36. Ks. myös Husa, Mutanen & Pohjolainen 2001, 13.
[8] Husa, Mutanen & Pohjolainen 2001, 13–14.
[9] Siltala 2003, 504; Hirvonen 2011, 7–8.

on merkitystä oikeudenkäytössä. Tutkimusmaailma on muokkautunut uudenlaiseen suuntaan, ja yhä enemmän jalansijaa saavat poikkitieteelliset tutkimukset, joiden avulla pyritään ratkaisemaan kompleksisia ongelmia, kuten rikollisuutta ja syrjäytymistä.[10] Empiiristä tutkimusta on tehty oikeudenalan parissa aiempaa runsaammin, ja sen asema on vahvistunut suomalaisessa oikeustutkimuksessa. Oikeustutkimuksen professori Kaijus Ervasti toteaakin, että ”oikeus on kaikkialla”. Täten oikeuden asema osana yhteiskuntaa on tärkeä huomioida, sillä se vaikuttaa jokaisen arkeen.[11]

Lainopillinen lähestymistapa valittiin opinnäytetyön suuntaa antavaksi menetelmäksi sen vuoksi, että se mahdollistaa aiheiden tarkastelun lain soveltamisen ja tulkitsemisen näkökulmasta. Tämä lähestymistapa on ollut avainasemassa lain yksityiskohtien, taustojen, tarkoitusten ja muutosten ymmärtämisessä sekä niiden käytännön vaikutusten arvioinnissa. Lisäksi oikeusdogmaattinen näkökulma korostaa oikeudellisen tiedon merkitystä ja lisää ymmärrystä tutkittavista aiheista oikeudellisesta näkökulmasta käsin. Tässä opinnäytetyössä tutkitaan identiteettivarkauksia ilmiönä, sen suhdetta kansalliseen lainsäädäntöön sekä rahanpesua ilmiönä ja siihen liittyvää kansainvälistä ja kansallista sääntelyä. Identiteettivarkauksia ja petosrikollisuutta käsittelevissä kappaleissa keskeisenä lähteenä toimii rikoslaki (39/1889). Lisäksi on hyödynnetty lähteinä lain esitöitä, kuten hallituksen esityksiä, lakivaliokunnan mietintöjä sekä muuta oikeuskirjallisuutta ja -tutkimusta. Tärkeän aseman muodostavat myös eri viranomaisten ja asiantuntijoiden tuottamat tiedot. Myös esimerkiksi rahanpesun sääntely pohjautuu pitkälti erilaisiin kansainvälisiin sekä eurooppaoikeudellisiin sopimuksiin ja velvoitteisiin. Pohjana sääntelylle toimivat YK:n (Yhdistyneiden Kansakuntien) yleissopimukset ja Financial Action Task Force -järjestön (FATF) standardit. Keskeisenä lähteenä rahanpesua käsittelevissä kappaleissa toimii myös Suomen rikoslaki (39/1889), lain esityöt, oikeuskirjallisuus ja -tutkimus sekä eri viranomaisten ja asiantuntijoiden tuottama tieto.

Menetelmänä lainopillinen näkökulma tutkimusaiheisiin on mahdollistanut soveltuvien rikoslain lukujen ja pykälien tulkinnan ottaen huomioon semantiikan. Pykälissä mainitut sanamuodot ja merkitykset on siten pyritty tulkitsemaan ja selittämään auki niin, että lainopillinen tavoite selvittää miten velvoittavan oikeuden mukaan tulisi toimia, täyttyisi. Tietyn tunnusmerkistön täyttävän toiminnan yksityiskohtaisempi tulkitseminen, toiminnan edellytykset, seuraamukset ja tosiasialliset toimintamallit oikeudellisesta näkökulmasta on käyty läpi hyödyntämällä rikoslakia, mutta myös lainopin ulkopuolisia, empiirisiä lähteitä hyödyntämällä. Hyödyntämällä kahta eri lähestymistapaa opinnäytetyössä käsiteltyjen aiheiden monimuotoisuus, yksityiskohdat ja toisaalta myös ilmiöiden näyttäytyminen yhteiskunnassa tulee mahdollisimman laajasti tutkimuksessa esiin pyrkien antamaan kattavan kuvauksen aiheista ja niiden

[10] Ervasti 2022, 7 & 12–13.
[11] Ervasti 2011, 66; Ervasti 2022, 5.

piirteistä. Opinnäytetyössä on otettu huomioon myös lakien ja ilmiöiden taustalla oleva historiallinen kehitys, sillä menneisyyden ymmärtäminen on olennaista nykytilanteen ja tulevien suuntausten hahmottamiseksi. Historiallisten tapahtumien ja päätösten tutkiminen tarjoaa myös syvempää tietoa siitä, miten nykyinen oikeudellinen ja yhteiskunnallinen järjestelmä käsiteltävien aiheiden osalta on muotoutunut ja miksi tietyt käytännöt ovat vallitsevia. Mahdollisimman laajan kuvauksen saamiseksi ja oikeusjärjestyksen systematisoinnin, eli jäsentämisen vuoksi myös käytetyt oikeudelliset termit ja käsitteet on pyritty selittämään kattavasti auki. Kuten oikeustieteellisessä tutkimuksessa yleisestikin, myös tässä opinnäytetyössä hyödynnetään siis useampaa eri menetelmää joustavasti ottaen huomioon myös juridiikan ulkopuolelle jäävät seikat.

3 Identiteettivarkaus ja sen asema kotimaisessa lainsäädännössä

Rikoslain (39/1889) 38 luvun 9 a §:n mukaan identiteettivarkaus on osa tieto- ja viestintärikoksia. Mainitun pykälän mukaan identiteettivarkaudesta on kyse silloin, kun joku erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee. Pykälän mukaan rangaistus identiteettivarkaudesta on sakkoa.

Identiteettivarkaus tarkoittaa rikosta, jossa rikoksentekijän tarkoituksena on erehdyttää kolmatta osapuolta käyttämällä toisen henkilötietoja, tunnistautumistietoja tai muuta yksilöivää tietoa. Ennen rikoslain kokonaisuudistusta säännösten vanhentuneisuus aiheutti epäselvyyttä rangaistuksien tulkinnan suhteen. Rikoslain kokonaisuudistuksen toisessa vaiheessa (HE 94/1993) uudistettiin lakia myös tieto- ja viestintärikoksien osalta, jotta laki vastaisi teknologian nopeaa kehitystä.[12] Lakivaliokunnan mietinnössä (LaVM 22/1994) rikoslain kokonaisuudistuksen toiseen vaiheeseen liittyen valiokunta arvosteli hallituksen esitystä siitä, etteivät rikoslain yleisen osan luvut (ts. yleiset opit)[13] sisältyneet esitykseen. Yleisten osien lukujen puuttuminen esityksestä aiheutti epävarmuutta syyksiluettavuutta ja rikokseen osallisuutta koskevien säännösten arvioinnin suhteen. Lisäksi käsitykset lainkonkurrenssista[14] ja rikosten

[12] HE 94/1993 vp, 1.
[13] Ks. Korkka-Knuts 2020, 4 & 10 mukaan Nuotio 1998, 30–38. Rikosoikeuden yleiset opit liittyvät oppijärjestelmänä rikosoikeuden teoreettiseen tutkimukseen. Laajemman määritelmän mukaan yleisiin oppeihin sisältyvät oikeusperiaatteet, teoriat, käsitteet, oikeuslähdeoppi ja metodioppi. Yleisten oppien tarkoituksena on luoda yhtenäinen viitekehys sääntelylle, jotta toiminnan tai sen laiminlyönnin kriminalisoinnin, rangaistavuuden sekä syyllisyyden ja tunnusmerkkien määritteleminen olisi loogista.
[14] Ks. Boucht & Frände 2019, 181. Lainkonkurrenssilla tarkoitetaan tilannetta, jossa yhteen tiettyyn rikolliseen toimintaan voisi soveltaa useampaa eri rikostunnusmerkistöä, eli toisin sanoen teko kattaisi joko kokonaan tai osittain useamman eri rikoksen tunnusmerkistön.

yhtymistä[15] koskevista säännöksistä vaihtelivat merkittävästi, ja valiokunnan mielestä seuranta tuomioistuinkäytännön yhdenmukaisuudesta oli tarpeen. Rikoslain kokonaisuudistuksen ensimmäisen vaiheen jälkeen valiokunta piti keskittämisperiaatteen[16] noudattamista suotavana myös uudistuksen toisessa vaiheessa. Keskittämisperiaatteen noudattaminen oli sujunut pääosin tehokkaasti, mutta jotkin rangaistavuuden kriteerit eivät olleet selkeästi määriteltyinä laissa, ja rangaistussäännökset olivat liian yleisluontoisia. Valiokunnan mukaan periaatteiden noudattaminen vaatisi tehokkaampaa yhteistyötä ministeriöiden välillä. Valiokunta puolsi tieto- ja viestintärikoksia koskevan luvun 38 hyväksymistä mietinnön mukaisesti.[17]

Identiteettivarkaus kriminalisoitiin vuonna 2015, ja yhtenä tavoitteena oli selkeyttää identiteettivarkauden uhriksi joutuneen asemaa. Lakiesityksen (HE 232/2014) tarkoituksena oli myös saattaa lainsäädäntö vastaamaan Euroopan parlamentin ja neuvoston direktiiviä tietojärjestelmiin kohdistuvista hyökkäyksistä (EU) 2013/40.[18] Direktiivin noudattamiseksi vaaditut lait, asetukset ja määräykset oli toimeenpantava jäsenvaltioissa viimeistään syyskuussa 2015.[19] Direktiivin tarkoituksena oli yhtenäistää jäsenvaltioiden rikosoikeudellisia säännöksiä ja edistää viranomaisten välistä yhteistyötä jäsenvaltioiden välillä. Lakivaliokunnan mietinnössä (LaVM 29/2014) todettiin, että verkkorikollisuuden toimintaympäristön muuttuessa nopeasti on tärkeää, että lainsäädäntö on ajantasainen ja kattava. Identiteettivarkauksien osalta valiokunta totesi nykylainsäädäntöä täydentävälle kriminalisoinnille olevan tarvetta. Selvityksen mukaan ennen esityksen hyväksymistä oli jo päässyt syntymään tilanteita, joissa rikoksentekijä olisi voitu tuomita identiteettivarkaudesta samalla kun vakavamman rikoksen tunnusmerkistö[20] ei olisi täyttynyt. Valiokunta puolsi identiteettivarkauden kriminalisointia hallituksen esittämällä tavalla mainiten kuitenkin, että pykälässä mainittujen ”tietojen” voitaisiin käsittää sisältävän myös tietoyhteiskuntakaaren (917/2014) 1 luvun 3 §:n 40 kohdassa

---

Samansuuntaisesti myös Luoto 2022, 403. Lainkonkurrenssilla tarkoitetaan tilannetta, jossa rikoksentekijän toiminta voi täyttää usean eri rikoksen tunnusmerkistön. Tilanteen ratkaisemiseksi voidaan joutua soveltamaan kaikkia soveltuvia tunnusmerkistöjä tai päättää, sovelletaanko jotain tiettyä tunnusmerkistöä muiden sijaan.

[15] Ks. Boucht & Frände 2019, 181. Rikosten yhtymisellä eli rikoskonkurrenssilla tarkoitetaan tilannetta, jossa on kyse siitä, onko rikoksentekijä tehnyt yhden vai useamman rikoksen ennen rangaistukseen tuomitsemista. Yleisesti katsotaan, että rikoksentekijä tuomitaan kaikista tekemistään rikoksista, mikäli kyseiset teot ovat rikkoneet useampaa rikostunnusmerkistöä eli rangaistussäännöstä. Ks. myös Luoto 2022, 405. Rikosten yhtymisessä voidaan esimerkiksi lainkonkurrenssista johtuen rikoksentekijän toimintaa tulkitakin ainoastaan yhdeksi rikokseksi.

[16] Ks. Matikkala 2013, 91. Keskittämisperiaatteen mukaan kaikki vankeusuhkaiset rangaistussäännökset tulee olla keskitettynä rikoslakiin. Sakonuhkaisia rangaistussäännöksiä voisi siten olla myös rikoslain ulkopuolella. Alaviitteessä 14 sivulla 97 Matikkala kuitenkin toteaa, että keskittämisperiaatteen täydellinen noudattaminen on hankalaa.

[17] LaVM 22/1994 vp, 5–6 & 69.

[18] HE 232/2014 vp, 1 & 38.

[19] 2013/40/EU.

[20] Ks. Andström 2003. Rikostunnusmerkistö määrittelee teon rangaistavan vääryyden. Rikollinen teko on siis oikeudenvastainen, syyllisyyttä osoittava ja tunnusmerkistön mukainen teko.

tarkoitetut välitystiedot. Lisäksi valiokunta ehdotti lausumaehdotuksen hyväksymistä: lausumassa vaadittiin, että hallitus valvoo identiteettivarkauksien tutkintakeinojen riittävyyttä.[21]

Identiteettivarkaudet tulevat esiin yleensä muun rikollisen toiminnan ohessa, kuten petoksien yhteydessä. Riippuen rikoksen konkreettisesta tekotavasta, teko voi täyttää myös esimerkiksi kunnianloukkauksen tai yksityiselämää loukkaavan tiedon levittämisen tunnusmerkistön.[22] Rikoslain 38 luvun 9 a §:n mukaan rangaistus identiteettivarkaudesta on sakko, eli rikoksena identiteettivarkaus on tasoltaan lievä. Tämä vaikuttaa viranomaisten käytössä oleviin keinoihin selvittää ja puuttua rikokseen. Identiteettivarkauden tapahtuessa osana muuta rikollista toimintaa, kuten petoksen yhteydessä, viranomaisten käytettäviin keinoihin voi sisältyä myös tutkimuksen kannalta välttämättömät pakkokeinot. Identiteettivarkautta itsenäisenä rikoksena tutkittaessa viranomaisten käytössä ovat myös poliisilain (872/2011) 4 luvun 3 §:ssä mainitut tiedonsaantikeinot. Kyseisen pykälän 2 momentin perusteella poliisilla on yksittäistapauksessa oikeus pyynnöstä saada teleyritykseltä ja yhteisötilaajalta yhteystiedot sellaisesta teleosoitteesta, jota ei mainita julkisessa luettelossa, taikka teleosoitteen tai telepäätelaitteen yksilöivät tiedot, jos tiedot ovat tarpeen poliisille kuuluvan tehtävän suorittamiseksi.[23] Lisäksi tutkinnassa voidaan käyttää lain sananvapauden käyttämisestä joukkoviestinnässä (460/2003) 17 §:n sisältämiä keinoja verkkoviestin tunnistamistietojen luovuttamiseen ja teon ollessa tehty teleosoitetta tai telepäätelaitetta hyödyntäen myös pakkokeinolain (806/2011) 10 luvun 7 §:ssä mainittua teleosoitteen tai telepäätelaitteen haltijan suostumuksella tapahtuvaa televalvontaa.[24]

Identiteettivarkauden rangaistavuuden edellytyksinä ovat teon tarkoituksenmukaisuus erehdyttämismielessä, toimiminen oikeudettomasti sekä henkilötietojen, tunnistamistietojen tai muun vastaavan yksilöivän tiedon käyttö. Erehdytetty ei tarkoita ainoastaan luonnollista henkilöä, vaan se voi tarkoittaa myös henkilöiden luomaa tai hallinnoimaa järjestelmää. Ratkaisevaa erehdyttämisessä on siis enemmänkin se, että kolmannen osapuolen erehdytys tapahtuu henkilöllisyyden tai identiteetin kautta. Oikeudettomasti taas tekijä ei toimi, jos hänellä on esimerkiksi oikeus käyttää tiettyä IP-osoitetta[25]. Henkilötiedoilla, tunnistamistiedoilla sekä muulla vastaavalla yksilöivällä tiedolla tarkoitetaan kaikkea sitä tietoa, minkä perusteella kolmas osapuoli voisi erehtyä uskomaan tiedon käyttäjän olevan se henkilö, jota tietojenkäyttö koskee. Aiemmin henkilötietoon sisältyi sittemmin kumotun henkilötietolain (523/1999) 3 §:n 1 kohdan mukaan kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai

[21] LaVM 29/2014 vp, 2–5.
[22] HE 232/2014 vp, 38.
[23] HE 232/2014 vp, 37–38. Ks. myös Kallio 2021, tiivistelmä.
[24] LaVM 29/2014 vp, 4.
[25] Ks. TEPA-termipankki 2024. IP-osoite on verkkoliittymän, tietojenkäsittely- tai tiedonsiirtolaitteen yksilöllinen numeerinen tunnus.

hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.[26] Tällä hetkellä henkilötietoja koskeva sääntely on Euroopan unionin yleisen tietosuoja-asetuksen (EU 2016/679) ja siitä pohjautuvan tietosuojalain (1050/2018) varassa. Yleinen tietosuoja-asetus (GDPR) tuli voimaan vuonna 2016 ja jäsenvaltiot alkoivat soveltamaan asetusta vuodesta 2018. Tietosuojalailla täydennettiin yleistä tietosuoja-asetusta ja sitä sovelletaan yhdessä tietosuoja-asetuksen kanssa.[27] Tunnistamistietoon sisältyy pakkokeinolain (806/2011) 10 luvun 6 §:n mukaan tilaajaan tai käyttäjään yhdistettävissä olevaa viestiä koskevaa tietoa, jota viestintäverkossa käsitellään viestin siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi. Tällaista tietoa voi olla esimerkiksi IP-osoite. Luonnollisen henkilön lisäksi pykälässä ilmaistulla ”toisella” voidaan tarkoittaa myös oikeushenkilöä. Pykälässä mainitun muun yksilöivän tiedon tarkoituksena on kattaa myös oikeushenkilön yksilöivät tiedot.[28]

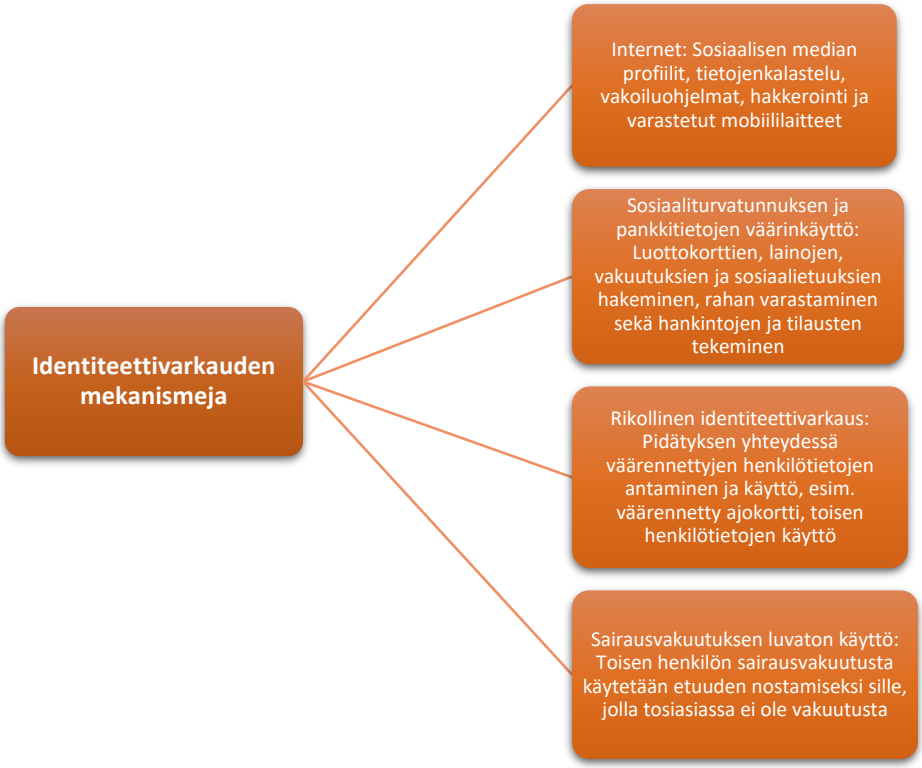
Rikoksen tunnusmerkistö ei täyty, jos todellista erehtymisen mahdollisuutta ei ole, toisen tietojen käyttö on hyvin vähäistä tai koskee kokonaisuuden kannalta irrallista seikkaa. Oleellista toisen tietojen käytössä on, että tiedot liittyvät tai kytkeytyvät henkilön tunnistamiseen ja siten johtaisivat erehtymiseen. Esimerkiksi, vaikka käytetty tieto olisikin sisällöltään henkilötietoa, se ei olisi merkityksellistä, ennen kuin se liittyy muuhun sellaiseen tietoon tai esiintyy sellaisessa yhteydessä, joka mahdollistaisi henkilön tunnistamisen. Erehtymisen mahdollisuutta ei myöskään ilmenisi, jos kyseessä olisi selkeästi satiiriksi tulkittava toiminta tai pseudonyymillä esiintyminen. Erehdyttämistarkoituksen puuttuessa teko ei ole rangaistava. Teon on myös oltava sellainen, että se on aiheuttanut asianomistajalle joko taloudellista vahinkoa tai jonkin muun kuin vähäisenä pidetyn haitan. Taloudellinen vahinko voi ilmetä erilaisina tilanteen selvittely- ja korjauskuluina. Haitta taas voi ilmetä tilanteen selvittämisen ja oikaisemisen hankaluutena tai sen epäonnistumisena. Esimerkiksi kun toisen henkilötietoja on käytetty petoksen tekemiseen, tilanteen ratkaiseminen voi edellyttää asianomistajalta merkittävää vaivannäköä. Myös sosiaaliseen mediaan toisen henkilötiedoilla luodun valeprofiilin poistaminen voi olla hankalaa. Internetissä tapahtuvien identiteettivarkauksien osalta korostuukin tietojen poistamisen tai korjaamisen haastavuus ja siten myös pykälässä mainittu vähäistä suurempi haitta.[29]

3.1 Identiteettivarkauden mekanismit

Omat raha-asiat, terveydenhoitoon liittyvät asiat ja monet muut palvelut hoidetaan nykyään pääasiassa digitaalisesti verkossa. Vastaavanlaisten arkaluonteisten tietojen päätyminen

[26] HE 232/2014 vp, 36.
[27] HE 9/2018 vp, 4–5.
[28] HE 232/2014 vp, 36–37.
[29] HE 232/2014 vp, 36–37.

vääriin käsiin voi aiheuttaa huomattavaa taloudellista sekä henkistä haittaa.[30] Vuonna 2016 poliisin tietoon tulleiden rikosten osalta identiteettivarkaus oli yleisin kyberrikollisuuden tekomuoto. Identiteettivarkaus paljastuu usein petosten tutkinnan yhteydessä.[31] Vaikka petostapauksissa omaisuuden takaisinsaannin mahdollisuudet ovat pienet kotimaassa ja vielä vähäisemmät ulkomailta käsin tapahtuvissa huijauksissa, niistä suositellaan tekemään rikosilmoitus. Tyypillistä tapauksissa on, että sama rikoksentekijä on huijannut myös muita uhreja ja ilmoitusten avulla tekijän tai tekijöiden kiinnijääntä on mahdollista. Myös kansainvälisen yhteistyön avulla on paljastettu ulkomaisia petosvyyhtejä. Identiteettivarkauteen tarvittavia tietoja saadaan suurimmaksi osaksi internetistä. Henkilö- tai pankkitiedot annetaan tyypillisesti epähuomiossa väärään paikkaan tai kerätään tietomurtojen yhteydessä.[32]



Kuvio 1: Identiteettivarkauden mekanismeja (mukaillen Kyberturvallisuuskeskus 2023, 1 & Poliisi 2024a)

Identiteettivarkaus pohjautuu useimmiten tarvittavien tietojen hankkimiseen esimerkiksi sosiaalisen median profiilien kautta, tietojen kalastelusivustoilta, vakoiluohjelmien sekä

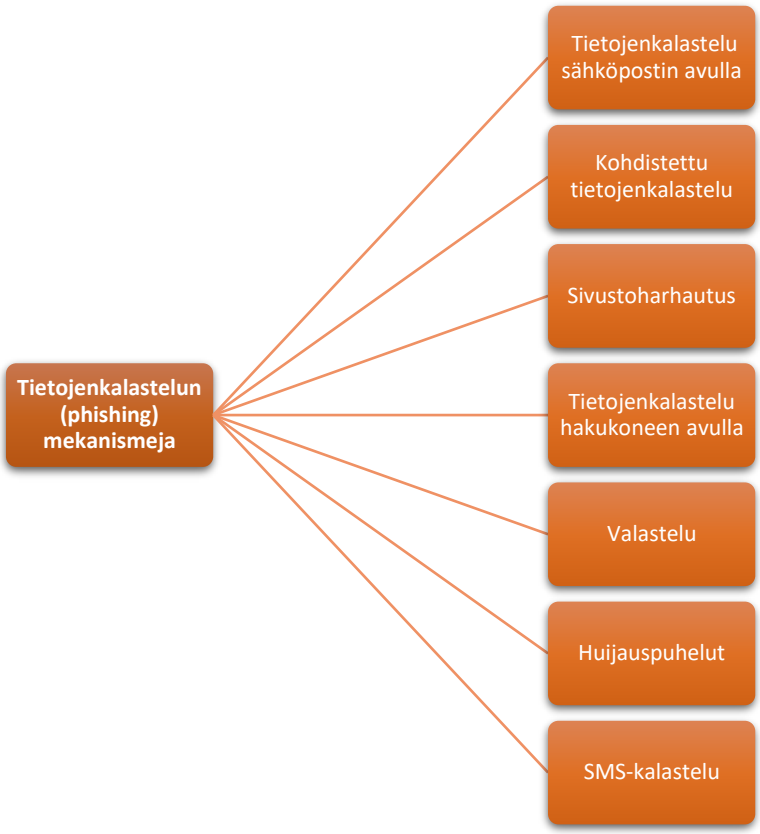
[30] Kyberturvallisuuskeskus 2023, 1.
[31] Näsi & Tanskanen 2017, 158.
[32] Poliisi 2024a.

hakkeroinnin avulla tai varastetusta mobiililaitteesta. Identiteettivarkauden kohteen nimen, osoitteen tai henkilötunnuksen hankkiminen ja käyttö voi riittää identiteettivarkauden toteuttamiseen.[33] Yleisimmin rikoksentekijän tarkoitusperänä on saavuttaa taloudellista hyötyä identiteettivarkauden avulla. Tällainen hyöty saavutetaan esimerkiksi uhrin sosiaaliturvatunnuksen ja pankkitietojen väärinkäytön kautta. Näiden tietojen avulla rikoksentekijä voi avata uhrinsa nimiin uusia luottokortteja, hakea lainaa tai sosiaalietuuksia, siirtää uhrin varallisuutta itselleen tai muille sekä tehdä muunlaisia tilauksia ja hankintoja uhrin nimissä. Rikollisella identiteettivarkaudella taas tarkoitetaan sellaista tilannetta, jossa rikoksentekijä antaa esimerkiksi pidätyksen yhteydessä väärän henkilötiedon ilmoittamalla olevansa joku toinen henkilö, antamalla väärän henkilötunnuksen tai esiintyy toisena henkilönä käyttämällä väärennettyä tai varastettua henkilöllisyystodistusta. Myös sairausvakuutuksen luvaton käyttö on identiteettivarkaudeksi luettava teko, vaikkakin se on Suomessa tekomuotona hyvin harvinainen. Tällaisessa tilanteessa rikoksentekijä nostaa toisen henkilön sairausvakuutuksen todellisuudessa omaan käyttöönsä, vaikka hän ei ole vakuutuksen saaja.[34] Perinteisissä identiteettivarkauksissa käytetään varastettuja tai uhrilta kadonneita ja sittemmin löydettyjä henkilötodistuksia tai varastetaan uhrin postia. Uhri saattaa myös epähuomiossa hävittää henkilötietoja sisältävää paperia jätteiden mukana.[35]

Henkilötietoja päätyy rikollisten käsiin myös eri kokoisissa organisaatioihin kohdistuvissa tietomurroissa. Tietomurtojen avulla saatuja henkilötietoja voidaan hyödyntää rikosten tekemisessä vuosienkin päästä tietomurrosta. Tietomurrolla viitataan sellaiseen tapahtumaan, jossa joku tunkeutuu oikeudettomasti tietojärjestelmään. Tietomurtoja tehdään tietojenkalastelun avulla sekä tunkeutumalla erilaisten turvajärjestelmien ohi.[36] Tietomurrosta säädetään rikoslain (39/1889) 38 luvun 8 §:ssä seuraavanlaisesti: Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen enintään kahdeksi vuodeksi. Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta 1) teknisen erikoislaitteen avulla tai 2) muuten teknisin keinoin turvajärjestelyn ohittaen, tietojärjestelmän haavoittuvuutta hyväksi käyttäen tai muuten ilmeisen vilpillisin keinoin oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta tai datasta. Myös tietomurron yritys on rangaistava teko.

[33] Poliisi 2024a.
[34] Kyberturvallisuuskeskus 2023, 1.
[35] Poliisi 2024a.
[36] Poliisi 2024a; Poliisi 2024b.

Tietomurtojen tyypillisin toteutustapa on kirjautumistietojen varastaminen, joka tapahtuu tyypillisesti tietojenkalastelun (phishing) avulla. Tietojenkalastelussa rikoksentekijä huijaa uhrin kirjautumistiedot käyttöönsä rikollisen toiminnan suorittamiseksi.[37] Tietojenkalastelun mekanismeja on useita.



Kuvio 2: Tietojenkalastelun mekanismeja (mukaillen Kyberturvallisuuskeskus 2023, 1)

Sähköpostin avulla tapahtuva tietojenkalastelu tapahtuu usein rikollisten esiintyessä hyvämaineisina yrityksinä, kuten tunnettuina ja luotettavina pankkeina. Tietojenkalasteluviestejä vastaanotetaan sähköpostiin, mobiilisovelluksiin sekä sosiaalisen median ja erilaisten verkkosivustojen kautta ja ne sisältävät esimerkiksi pankin nimissä tehdyn väärennetyn turvallisuusvaroituksen, jonka avulla pyydetään uhrin käyttäjätunnusta ja salasanaa. Kohdistettu tietojenkalastelu tarkoittaa tiettyyn henkilöön, ryhmään tai yritykseen kohdistuvaa tietojenkalastelua, joka tapahtuu tyypillisesti sähköpostin tai verkkosivujen kautta. Esimerkiksi tietyn yrityksen työntekijät voivat vastaanottaa sähköpostiinsa erilaisia liitetiedostoja, jotka ladatessa tai avatessa keräävät kirjautumistietoja käyttäjän tietokoneelta. Sivustoharhautus tapahtuu verkkosivustojen ja tietokoneiden avulla, esimerkiksi uhrin käyttäessä oman pankkinsa nettisivuja. Sivustolle voi ilmaantua esimerkiksi ilmoitus etäkirjautumisesta, jossa pyydetään uhrin

[37] Poliisi 2024b.

henkilötietoja vedoten valheellisesti siihen, että uhrin tiedot ovat päätyneet varastetuiksi. Tietojenkalastelu hakukoneen avulla tarkoittaa sellaista tilannetta, jossa hakkerit ovat luoneet aidonoloisen sivuston, joka on päätynyt laillisiin hakukoneisiin. Uhrin hakiessa hakukoneesta esimerkiksi viranomaisten sivuja, hakutuloksiin on päätynyt väärennettyjä viranomaisten sivustoja, joihin kirjautuminen vaarantaa uhrin tiedot. Valastelu[38] tarkoittaa rikollisten esiintymistä luotettavina tai tunnettuina toimijoina rahallisen hyödyn tai tietojen saamiseksi korkean tason johtajilta. Valastelu tapahtuu usein sosiaalisen median tai sähköpostin kautta, ja viestin liitteenä olevat tiedostot sisältävät mitä tahansa arvokasta tietoa keräävän haittaohjelman. Huijauspuhelut tapahtuvat nimensä mukaisesti puhelimen tai muiden langattomien laitteiden avulla. Puheluiden tarkoituksena on kerätä tai varastaa rahaa ja arkaluonteisia tietoja harhauttamalla uhria esiintyen toisena tahona, esimerkiksi pankin työntekijänä. SMS-kalastelu tapahtuu langattomien laitteiden avulla. Tyypillisesti uhri saa tekstiviestin esimerkiksi arpajaisvoitosta, myöhässä olevasta laskun maksusuorituksesta tai saapuneesta postilähetyksestä. Viestin sisältämän linkin avatessaan uhrin laitteelle asentuu erilaisia haittaohjelmia.[39]

3.2 Identiteettivarkaudet osana kyberrikollisuutta ja yleisyys Suomessa

Kyberrikollisuus tarkoittaa tietoverkkovälitteistä ja verkossa tapahtuvaa rikollisuutta. Termi ei ole rikosoikeudesta peräisin, vaan yleisesti käytetty ilmaisu kaikenlaiselle verkossa tapahtuvalle rikolliselle toiminnalle. Kyberrikollisuus jaotellaan tietoverkkosidonnaisiin (cyber dependent) rikoksiin ja tietoverkkoavusteisiin (cyber enabled) rikoksiin. Tietoverkkosidonnaiset rikokset kohdistuvat nimensä mukaisesti tietoverkkoihin tai -järjestelmiin, ja rikoksen tekeminen vaatii tietoverkkojen ja tietokoneiden hyödyntämistä rikollisen toiminnan toteuttamiseksi. Esimerkiksi tietomurrot kuuluvat tietoverkkosidonnaisten rikoksien kategoriaan. Tietoverkkoavusteisissa rikoksissa tietoverkot ja -järjestelmät mahdollistavat perinteistenkin rikoksien, kuten rahanpesun, tekemisen, mutta rikokset eivät suoraan kohdistu tietoverkkoihin tai -järjestelmiin.[40] Tieto- ja viestintärikokset on esitetty taulukossa 1.

Tieto- ja viestintärikokset (RL 38)
Salassapitorikos 38:1.1/1–2
Salassapitorikkomus 38:2.1–2
Viestintäsalaisuuden loukkaus 38:3.1/1–2
Viestintäsalaisuuden loukkauksen yritys 38:3.2

[38] Ks. TEPA-termipankki 2016. Valastelu (whaling) tarkoittaa johtavassa tai muuten tärkeässä asemassa olevaan henkilöön kohdistuvaa verkkourkintaa.
[39] Kyberturvallisuuskeskus 2023, 1. Ks. myös YLE 2020.
[40] Näsi 2022, 128–129; Poliisi 2024c.

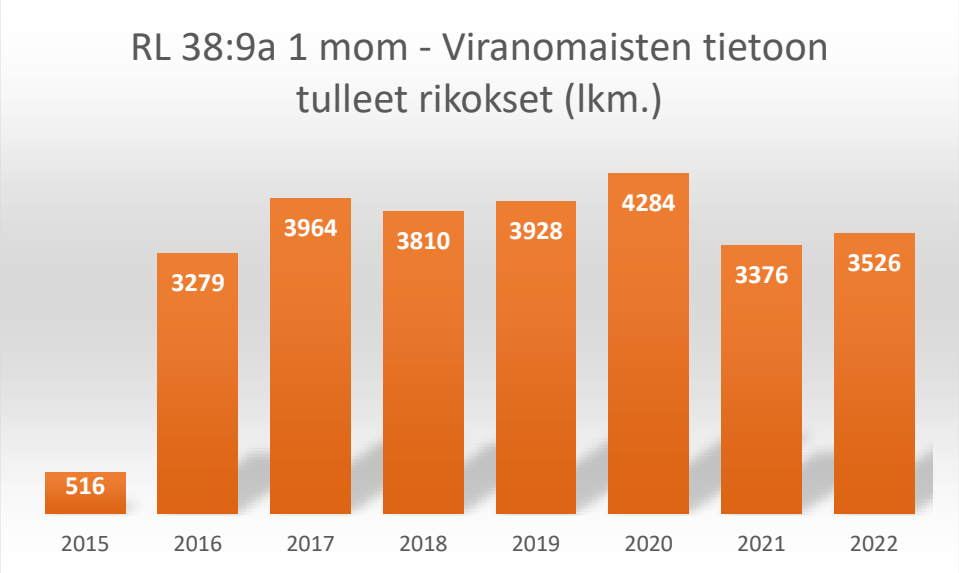
Törkeä viestintäsalaisuuden loukkaus 38:4.1/1–3
Viestintäsalaisuuden törkeän loukkauksen yritys 38:4.2
Tietoliikenteen häirintä 38:5.1
Tietoliikenteen häirinnän yritys 38:5.2
Törkeä tietoliikenteen häirintä 38:6.1/1–6
Tietoliikenteen törkeän häirinnän yritys 38:6.2
Lievä tietoliikenteen häirintä 38:7.1
Tietoliikenteen lievän häirinnän yritys 38:7.2
Tietojärjestelmän häirintä 38:7a.1
Tietojärjestelmän häirinnän yritys 38:7a.2
Törkeä tietojärjestelmän häirintä 38:7b.1/1–5
Tietojärjestelmän törkeän häirinnän yritys 38:7b.2
Tietomurto 38:8.1–2
Tietomurron yritys 38:8.3
Törkeä tietomurto 38:8a.1/1–2
Törkeän tietomurron yritys 38:8a.2
Suojauksen purkujärjestelmärikos 38:8b
Tietosuojarikos 38:9.1/1–3
Identiteettivarkaus 38:9a.1

Taulukko 1: Tieto- ja viestintärikokset (RL 38)

Erityyppisillä verkossa tapahtuvilla rikoksilla on erilaiset riskitekijänsä. Riski joutua kyberrikollisuuden uhriksi kasvaa, jos verkon ja teknologian käyttö on aktiivista. Toisaalta taas verkon ja teknologian edistyneet käyttötaidot eivät suojaa kyberrikollisuuden uhriksi joutumiselta. Myös aiempi ns. offline uhriksi[41] joutuminen on riskitekijä myös online uhriksi joutumiselle. Vaikka heikompi sosioekonominen tausta on yleensä ollut riskitekijä offline uhriksi joutumiselle, sama ei päde online uhriksi joutumisen riskeihin. Hyvä taloudellinen tilanne on riskitekijä kyberrikollisuuden erilaisten uhkien kokemiselle huolimatta henkilön iästä tai toiminnasta verkossa ja teknologian parissa. Myös vanhemmat miehet ovat enemmän alttiita

[41] Ks. Hakkarainen 2020, 19. Offline uhriksi joutumisella tarkoitetaan internetin ulkopuolella tapahtuvien rikoksien uhriksi joutumista.

huijauksille sekä haittaohjelmien toiminnalle.[42] Viranomaisten tietoon tulleiden rikosten osalta identiteettivarkaudet ovat yleisimpiä kyberrikollisuuden muotoja.[43] Taulukossa 2 on esitetty viranomaisten tietoon tulleet identiteettivarkaudet vuosina 2015–2022.



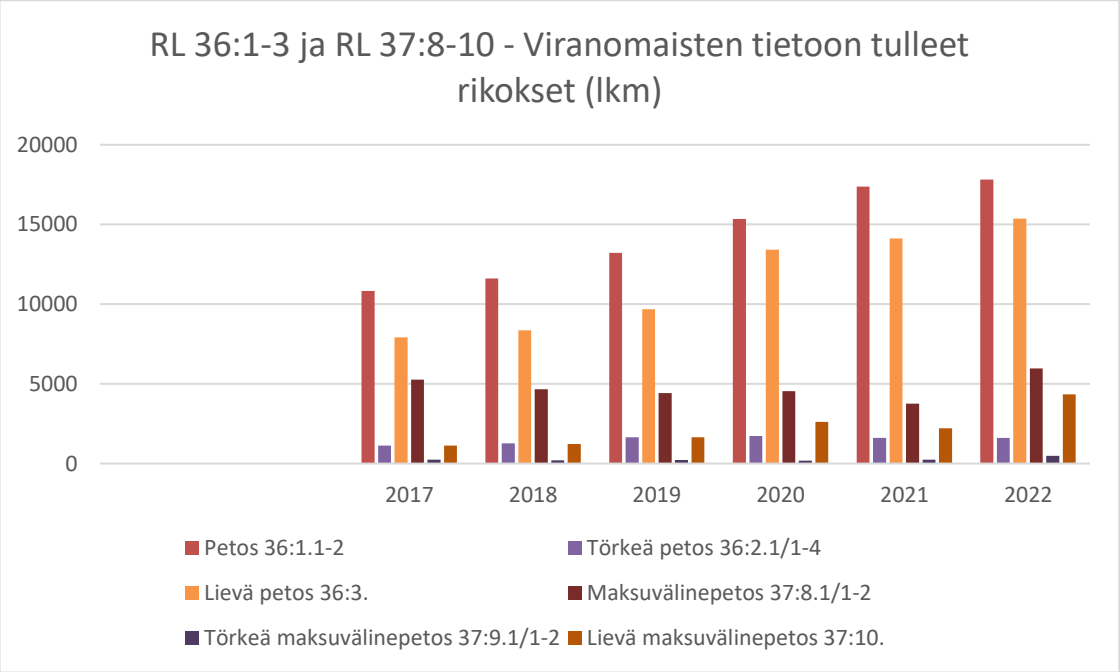
Taulukko 2: Viranomaisten tietoon tulleet identiteettivarkaudet vuosina 2015–2022[44]

Identiteettivarkauden kriminalisointivuonna 2015 viranomaisten tietoon tuli 516 identiteettivarkautta. Luku on suuri verrattuna muihin viranomaisten tietoon tulleisiin tieto- ja viestintärikoksiin. Toiseksi yleisimpänä kyberrikollisuuden muotona samana vuonna olivat perusmuotoiset tietomurrot, joita tuli viranomaisten tietoon yhteensä 341. Myös tietomurtojen määrä on kasvanut tasaisesti vuodesta 2015 eteenpäin, ja vuonna 2022 viranomaisten tietoon tuli jo 1846 tietomurtorikosta. Muiden tieto- ja viestintärikosten lukumäärä pysyi kymmenien tai satojen paikkeilla.[45] Identiteettivarkauksien määrä on kasvanut rajusti ja se on kyberrikollisuuden yleisin esiintymismuoto Suomessa. Identiteettivarkaudet ovat usein myös kytköksissä maksuvälinepetoksiin.[46]

Kansallisen rikosuhritutkimukseen perustuvan raportin mukaan miehistä 0,5 % ja naisista 0,7 % oli joutunut henkilötietojen väärinkäytön uhriksi koko elämänsä aikana ja vuoden 2021 aikana. Yleisin ikäluokka henkilötietojen väärinkäytön uhriksi joutuneille oli 35–54-vuotiaat. Maksukorttipetoksien uhriksi miehistä oli joutunut 2,0 % ja naisista 1,9 %. Samaisen raportin mukaan vastaajista yhteensä noin seitsemän prosenttia oli elämänsä aikana kokenut

[42] Näsi, Danielsson & Kaakinen 2022, 295–297.
[43] Näsi 2022, 134.
[44] Tiedot kerätty StatFinista.
[45] Tiedot kerätty StatFinista.
[46] Näsi 2022, 134.

taloudellista haittaa verkkorikollisuuden vuoksi. Vastaajat määrittelivät taloudellisen vahingon olleen aina muutamista euroista jopa satoihin tuhansiin euroihin asti. Vanhimpaan ikäryhmään, 55–74 vuotiaisiin kuuluvat ilmoittivat euromääräisesti suurimmat haitat, vaikka verkkorikoksen uhriksi joutuminen tässä ikäluokassa olikin harvinaisempaa. Vuoden 2021 aikana erinäiset huijausyritykset olivat myös raportin mukaan yleisiä, mutta taloudellista haittaa ei ollut päässyt juurikaan syntymään huijausyrityksien seurauksena. Yleisimpiin huijausyrityksiin kuuluivat mm. postihuijaukset, pankkihuijaukset ja sijoituspetokset.[47] Kuviossa 3 on kuvattu viranomaisten tietoon tulleita petosrikoksia vuosilta 2017–2022.



Taulukko 3: Viranomaisten tietoon tulleita petosrikoksia vuosilta 2017–2022[48]

Petosrikollisuus on kasvanut vuodesta 2010 alkaen, ja yhtenä selittävänä tekijänä pidetään tietotekniikan kasvanutta käyttöä ja sen kehitystä.[49] Erityisesti internetin avulla toteutettavat petokset ovat olleet yleinen keino petosrikosten toteuttamiseen, sillä riski kiinnijäämiseen on usein pieni ja saatava mahdollinen taloudellinen hyöty taas suuri. Lisäksi uhriksi voi tällöin valita kaukanakin asuvan henkilön, ja usein petosten tekijät toteuttavatkin tekojaan sarjoina kohdistuen useisiin uhreihin. Useilta eri uhreilta saadut taloudelliset hyödyt ovat usein huomattaviakin, vaikka yksittäisten uhrien kokema taloudellinen vahinko ei usein ole suurta. Huomattava osa petosrikoksista jää kuitenkin todennäköisesti viranomaisilta piiloon.

[47] Kolttola & Näsi 2022, 30–32.
[48] Tiedot kerätty Statfinista.
[49] Tanttari & Alanko 2017, 12.

Rikosilmoitusten teko olisi kuitenkin merkittävää siltä osin, että saatujen tietojen avulla viranomaisten on helpompi valvoa tällaisia rikosilmiöitä sekä puuttua niihin.[50]

Perusmuotoisten petoksien määrä on kasvanut vuodesta 2017 vuoteen 2022 noin 65 %, törkeiden petosten määrä taas 42 %. Merkittävintä tarkastelun alaisista petosrikoksista on kuitenkin lievien petosten kasvu: 94 %. Taulukossa 3 tarkastelunalaisena olevat rikosnimikkeet lievä petos, petos ja törkeä petos ovat rikoslain (39/1889) 36 luvun mukaan osa petoksia ja muuta epärehellisyyttä. 36 luvun 1 §:n mukaan petoksella tarkoitetaan tilannetta, jossa joku hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä taikka toista vahingoittaakseen, erehdyttämällä tai erehdystä hyväksi käyttämällä saa toisen tekemään tai jättämään tekemättä jotakin ja siten aiheuttaa taloudellista vahinkoa erehtyneelle tai tämän eduista määrääjälle. Toisen momentin mukaan petoksesta tuomitaan myös se, joka 1 momentissa mainitussa tarkoituksessa dataa syöttämällä, muuttamalla, tuhoamalla tai poistamalla taikka tietojärjestelmän toimintaan muuten puuttumalla saa aikaan tietojenkäsittelyn lopputuloksen vääristymisen ja siten aiheuttaa toiselle taloudellista vahinkoa. Rangaistus perusmuotoisesta petoksesta on sakkoa tai enintään kaksi vuotta vankeutta. Myös petoksen yritys on rangaistava teko. 36 luvun 2 §:n mukaan törkeästä petoksesta on kyse silloin, kun petoksessa tavoitellaan huomattavaa hyötyä, aiheutetaan huomattavaa tai erityisen tuntuvaa vahinkoa, rikos tehdään käyttämällä hyväksi vastuulliseen asemaan perustuvaa erityistä luottamusta tai rikos tehdään käyttämällä hyväksi toisen erityistä heikkoutta tai muuta turvatonta tilaa ja petos on myös kokonaisuutena arvostellen törkeä. Rangaistus törkeästä petoksesta on vähintään neljä kuukautta ja enintään neljä vuotta vankeutta. Myös törkeän petoksen yritys on rangaistava teko. Samaisen luvun 3 §:n mukaan lievästä petoksesta taas on kyse silloin, kun petos, huomioon ottaen tavoitellun hyödyn tai aiheutetun vahingon määrä taikka muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen. Rangaistus lievästä petoksesta on sakkoa.

Maksuvälinepetoksien kasvu vuodesta 2017 vuoteen 2022 on ollut noin 13 %, ja törkeiden maksuvälinepetoksien kasvu taas noin 94 %. Lievien maksuvälinepetoksien kasvu on ollut voimakasta: noin 285 %. Rikoslain (39/1889) 37 luvun 8 §:n mukaan maksuvälinepetoksesta on kyse silloin, kun joku hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä käyttää maksuvälinettä ilman sen laillisen haltijan lupaa, lupaan perustuvan oikeutensa ylittäen tai muuten ilman laillista oikeutta, käyttää väärää tai väärennettyä maksuvälinettä tai maksuvälineeseen liittyvää dataa syöttämällä, muuttamalla, tuhoamalla, vahingoittamalla, siirtämällä tai poistamalla taikka tietojärjestelmän toimintaan muuten puuttumalla saa aikaan rahan tai rahan arvon siirron lopputuloksen vääristymisen ja siten aiheuttaa toiselle taloudellista vahinkoa. Maksuvälinepetoksesta tuomitaan myös se, joka tilin katteen tai sovitun enimmäisluottorajan ylittäen väärinkäyttää 1 momentissa tarkoitettua maksuvälinettä ja siten aiheuttaa

[50] Tanttari & Alanko 2017, 12, 14–16.

toiselle taloudellista vahinkoa, jollei hänellä maksuvälinettä käyttäessään ollut aikomus viipymättä korvata vahinko. Ainoastaan ensimmäisen momentin kolmannen kohdan yritys on rangaistava teko. Rangaistus maksuvälinepetoksesta on sakkoa tai enintään kaksi vuotta vankeutta. 37 luvun 9 §:n mukaan törkeästä maksuvälinpetoksesta on kyse silloin, kun maksuvälinepetoksessa aiheutetaan huomattavaa tai erityisen tuntuvaa vahinkoa, rikos tehdään erityisen suunnitelmallisesti tai rikos tehdään osana 6 luvun 5 §:n 2 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa ja maksuvälinepetos on myös kokonaisuutena arvostellen törkeä. Ensimmäisen momentin kolmannen kohdan yritys on myös rangaistava teko. Rangaistus törkeästä maksuvälinepetoksesta on vähintään neljä kuukautta ja enintään viisi vuotta vankeutta. Samaisen luvun 10 §:n mukaan lievästä maksuvälinepetoksesta on kyse silloin, kun maksuvälinepetos, huomioon ottaen tavoitellun hyödyn tai aiheutetun vahingon määrä taikka muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen. Rangaistus lievästä maksuvälinepetoksesta on sakkoa.

Petoksista aiheutuvia haittoja voidaan välttää kansalaisten tietoisuuden ja tarkkaavaisuuden lisäämisellä. Eri mediat ja kanavat välittävät tietoa petosrikollisuudesta, ja merkittävissä asemissa onkin esimerkiksi poliisin ja pankkien viestintä ja tiedotus. Poliisi on kehittänyt kohderyhmäviestintäänsä sekä yhteistyötään eri medioiden kanssa entistä suunnitelmallisemmaksi, jotta viestintä tavoittaa myös tehokkaammin esimerkiksi ikääntyneet kansalaiset. Pankkien tehtäviin kuuluu mm. valvoa epäilyttävää rahaliikennettä, jolloin petoksien havaitseminenkin on mahdollista. Lisäksi pankin työntekijöille on erilaisia ohjeistuksia esimerkiksi taloudellisen hyväksikäytön tunnistamiseen.[51]

4 Rahanpesu ja sen asema kotimaisessa lainsäädännössä

Rikoslain (39/1889) 32 luvun 6 §:n mukaan rahanpesu on osa kätkemis- ja rahanpesurikoksia. Mainitun pykälän mukaan rahanpesusta on kyse silloin, kun joku ottaa vastaan, käyttää, muuntaa, luovuttaa, siirtää, välittää tai pitää hallussaan rikoksella hankittua omaisuutta, rikoksen tuottamaa hyötyä tai näiden tilalle tullutta omaisuutta hankkiakseen itselleen tai toiselle hyötyä tai peittääkseen tai häivyttääkseen hyödyn tai omaisuuden laittoman alkuperän tai avustaakseen rikoksentekijää välttämään rikoksen oikeudelliset seuraamukset. Rahanpesusta on kyse myös silloin, kun joku peittää tai häivyttää rikoksella hankitun omaisuuden, rikoksen tuottaman hyödyn taikka näiden tilalle tulleen omaisuuden todellisen luonteen, alkuperän, sijainnin tai siihen kohdistuvat määräämistoimet tai oikeudet taikka avustaa toista tällaisessa peittämisessä tai häivyttämisessä. Pykälän mukaan rangaistus rahanpesusta on sakkoa tai enintään kaksi vuotta vankeutta. Myös rahanpesun yritys luetaan rangaistavaksi teoksi.

[51] Tanttari & Alanko 2017, 17–19.

Rahanpesun ja kätkemisrikoksen ero muodostuu ainoastaan siitä seikasta, että kätkemisrikoksen esirikokset[52] ovat lueteltu laissa, mutta rahanpesun esirikoksia ei ole rajoitettu.[53]

Törkeästä rahanpesusta on kyse rikoslain (39/1889) 32 luvun 7 §:n mukaan silloin, kun rahanpesussa rikoksen kautta saatu omaisuus on erittäin arvokas tai rikos on tehty erityisen suunnitelmallisesti. Teon tulee myös olla kokonaisuutena arvostellen törkeä. Pykälän mukaan rangaistus törkeästä rahanpesusta on vankeutta neljästä kuukaudesta kuuteen vuoteen. Myös törkeän rahanpesun yritys luetaan rangaistavaksi teoksi. Rahanpesu muuttuu törkeäksi silloin, kun kyse on euromääräisesti noin 13 000 euron taloudellisesta hyödystä.[54] Tuottamuksellisesta rahanpesusta on kyse rikoslainlain (39/1889) 32 luvun 9 §:n mukaan silloin, kun joku törkeästä huolimattomuudesta ryhtyy 6 §:ssä tarkoitettuihin toimiin. Pykälän mukaan rangaistus tuottamuksellisesta rahanpesusta on sakkoa tai enintään kaksi vuotta vankeutta.

Edellä mainituissa pykälissä esiintyvät ilmaisut ”rikoksella hankittu omaisuus”, ”rikoksen tuottama hyöty” ja ”rikoksen kautta saatu omaisuus” ilmentävät sitä, että rahanpesu rikoksena edellyttää ensin toisen rikoksen tekemistä hyödyn saavuttamiseksi, nk. esirikosta. Tällöin myös syyttäjän on kyettävä näyttämään toteen esirikos ja siitä saavutettu taloudellinen hyöty, ja tätä vastuuta nimitetään esirikoksen yksilöinti- tai konkretisointivaatimukseksi[55]. Rahanpesusta tuomitsemisen ehtona ei tarvitse kuitenkaan olla esirikoksen tekijän tuomitseminen rangaistukseen esirikoksesta, eikä edes se, että esirikoksen tekijä olisi tiedossa. Tämä konkretisoituisi esimerkiksi sellaisessa tilanteessa, jossa rikollisjärjestössä rahanpesijöinä toimivat henkilöt ostaisivat huutokaupassa taidetta suurilla summilla. Heitä voitaisiin syyttää rahanpesusta, vaikka itse rikollisjärjestön jäseniä ei olisi vielä tuomittukaan mitään rikoksesta. Syyttäjä kykenisi tässä tapauksessa osoittamaan, että huutokaupassa käytetyt varat ovat peräisin laittomasta toiminnasta, koska ostajina ovat rikollisjärjestön rahanpesijät. Tällöin esirikoksen kriteerit täyttyvät. Huomionarvoista on myös se, että esirikoksen vanhentuminen ei estä syyttämistä ja tuomitsemista rahanpesusta, mutta rahanpesu voi vanhentua riippumatta esirikoksesta.[56]

Helsingin hovioikeudessa vuosina 2019–2022 törkeiden rahanpesurikosten esirikoksista yleisimpiä ovat olleet petosrikokset (9 kpl) ja huumausainerikokset (3 kpl). Muita esirikoksia törkeälle rahanpesulle ovat olleet veropetokset, velallisrikokset, varkaudet ja kavallukset.[57]

---

[52] Ks. Sahavirta 2008, 3. Ks. myös Heikkilä 2022, 7. Esirikoksella tarkoitetaan rikoshyötyä tuottavaa rikollista toimintaa, johon rahanpesu kohdistuu. Mikä tahansa taloudellista hyötyä tuottava rikos voi olla rahanpesun esirikos.
[53] HE 53/2002 vp, 34.
[54] HE 53/2002 vp, 36.
[55] Ks. Hyttinen 2017, 834. Yksilöinti- ja konkretisointivaatimuksilla pyritään selvittämään mistä rahat ovat peräisin, eli ts. määrittämään likaisen rahan alkuperä.
[56] Hyttinen 2017, 834. Ks. myös HE 53/2002 vp, 36.
[57] Heikkilä 2022, 10.

Rahanpesutuomioiden määrä vuosina 2015 ja 2016 oli yhteensä 229, ja vuosina 2017 ja 2018 tuomioiden määrä kasvoi 409:ään. Törkeisiin rahanpesuihin liittyvien syytekohtien määrä kasvoi vuosista 2015–2016 vuosiin 2017–2018 asti noin 104 %. Tällöinkin yleisimpiä esirikoksia olivat petosrikokset.[58] Vuonna 2007 julkaistussa Rahanpesun selvittelykeskuksen tutkimuksessa tarkasteltiin 61 rahanpesuun liittyvää tuomiota vuosien 1994–2006 väliseltä ajalta. Useimmissa tapauksissa rahanpesun esirikoksena oli ollut huumausaine tai talousrikos: puolessa tapauksista huumausainerikos oli esirikoksena. Talousrikoksista tyypillisimpiä esirikoksia olivat velallisen petos, velallisen epärehellisyys, veropetos, avustuspetos ja kavallus. Muina esirikoksina toimivat ryöstö, varkaus, maksuvälinepetos, perusmuotoinen petos ja kiskonta. Yhdessä tapauksessa oli kyse laittomaan tuontitavaraan ryhtymisestä ja kahdessa tapauksessa kyse oli ammattimaisesta alkoholipitoisen aineen salakuljetuksesta.[59]

Rahanpesu kriminalisoitiin aluksi rikoslain 32 luvun 1 §:n 2 momentissa (1304/1993) kätkemisrikoksena.[60] Säännös tuli voimaan vuonna 1994.[61] Rahanpesun kriminalisointi pohjautui pitkälti eurooppaoikeudellisten ja kansainvälisten velvoitteiden noudattamiseen, kuten vuonna 1988 tehtyyn Wienin huumausainesopimukseen ja 1990 tehtyyn Strasbourgin konfiskaatiosopimukseen. Wienin huumausainesopimus velvoitti rahanpesun kriminalisoimisen ainoastaan huumausainerikollisuuden osalta, kun taas Strasbourgin konfiskaatiosopimuksessa kriminalisointia ei sidottu koskemaan ainoastaan tiettyjä esirikoksia. Kriminalisointiin velvoitti myös vuoden 1991 rahanpesudirektiivi (91/308/ETY). Rikoslain 32 luvun 1 §:n 2 momentti, eli rahanpesusäädös (1304/1993), säädettiin näiden yleissopimusten vaatimusten täyttämiseksi. Tarve kriminalisoinnille syntyi järjestäytyneen huumausainerikollisuuden kautta.[62] Nykyäänkin sääntelyn perustana ovat Yhdistyneiden Kansakuntien (YK) yleissopimukset ja Financial Action Task Force -järjestön (FATF) standardit. Myös Euroopan Unionin rahanpesudirektiivien perusta pohjautuu FATF:n suosituksiin ja standardeihin.[63]

Rahanpesu kriminalisoitiin itsenäisenä rikoksena vuonna 2003 (61/2003) perustuen hallituksen esitykseen (HE 53/2002). Samalla korotettiin rahanpesurikosten rangaistuksia ja rangaistavaksi säädettiin myös rahanpesun yritys, salahanke törkeän rahanpesun tekemiseksi, tuottamuksellinen rahanpesu ja rahanpesurikkomus. Muutoksia perusteltiin järjestäytyneen rikollisuuden torjumisella ja muiden maiden lainsäädännön vastaavuudella. Lisäksi esityksessä huomautettiin, että yksittäisen maan suppeampi lainsäädäntö liittyen rahanpesurikoksiin voisi houkuttaa maahan entistä enemmän rikollista toimintaa. Lisäksi vuoden 1994 lakia sovellettaessa oli tullut epäselvyyksiä 1 momentin ja 2 momentin (rahanpesusäädös) käytön välillä:

---

[58] Salomaa 2019, 2.
[59] HE 285/2010 vp, 4–5.
[60] Sahavirta 2008, 4.
[61] HE 53/2002 vp, 4.
[62] HE 53/2002 vp, 7. Ks. myös Sahavirta 2008, 3 ja 7.
[63] Heikkilä 2022, 6; Finanssivalvonta 2024a.

vuosien 1994–1999 välisenä aikana rahanpesusäännöksen perusteella oli tuomittu yhteensä 36 henkilöä, mutta tosiasiassa vain 15 näistä oli sellaisia, jotka todellisuudessa olisi laskettu rahanpesuksi. Lisäksi 1 momenttiin sisältyi selkeästi määritellyt esirikokset, mutta tulkintavirheistä johtuen esirikosten listaa oli sovellettu myös 2 momentin mukaisiin rikoksiin.[64]

Rikoslain (39/1889) 32 luvun 6 §:ssä mainittu ”rikoksen tuottama hyöty” ulottuu sellaisiin tilanteisiin, joissa omaisuus on voitu hankkia laillisin keinoin. Lisäys on tehty sen vuoksi, että ”rikoksella hankitun omaisuuden” käsite ei itsessään kata verorikoksia ja velallisen rikoksia, vaikka esimerkiksi Strasbourgin konfiskaatiosopimuksen (1990) 6 artiklassa velvoitetaankin, että rahanpesun esirikosten joukko on rajoittamaton. Jos esimerkiksi laillisessa elinkeinotoiminnassa olisi toiminnasta syntyneitä verovelvoitteita laiminlyöty, niin laillisesta toiminnasta kertynyttä omaisuutta ei olisi oikeastaan hankittu rikoksen avulla, sillä kyseessä olisi tosiaankin laillisen elinkeinotoiminnan harjoittaminen. Ainoastaan omaisuuden jääminen rikoksentekijän haltuun olisi veropetoksen (esirikoksen) ansiota. Tällöin kaikenlainen rikoshyöty voi olla kohteena rahanpesulle. Jos siis verojen tilittämättä jättäminen täyttäisi rikoslain 29 luvun 4 §:ssä säädetyn verorikkomuksen tunnusmerkistön, voisi siitä saatu taloudellinen hyöty olla konfiskoinnin kohde.[65]

Rikoslain (39/1889) 32 luvun 6 §:n 1 momentin 1 kohdan mukaan rangaistavaa on ottaa vastaan, käyttää, muuntaa, luovuttaa, siirtää, välittää tai pitää hallussa rikoksella hankittua omaisuutta, rikoksen tuottamaa hyötyä tai näiden tilalle tullutta omaisuutta tiettyihin tarkoituksiin tietoisena omaisuuden tai varallisuuden alkuperästä. Käyttämisellä viitataan usein varallisuuden tai omaisuuden nopeaan tuhlaamiseen. Välittäminen koskee myös sellaista tilannetta, jossa rikoksentekijä ei saa varallisuutta haltuunsa vaan toimii esimerkiksi välittäjänä arvopaperikaupassa. Omaisuuden laittoman alkuperän peittämisellä ja häivyttämisellä tarkoitetaan usein omaisuuden siirtämistä, kätkemistä tai muuntamista johonkin toiseen muotoon, esimerkiksi varallisuuden siirtämistä bulvaanin[66] nimiin. Tunnusmerkistö täyttyy jo, kun varallisuutta on otettu vastaan, vaikka varsinaisiin peittely- tai häivyttämistoimiin ei olisi vielä ryhdytty. Peittämistä ja häivyttämistä voi siis olla varallisuuden tai omaisuuden säilyttäminen tai vastaanottaminen, sillä varallisuuden tai omaisuuden siirto pois alkurikoksentekijältä voi jo johtaa siihen, että varallisuuden todellista alkuperää ei saataisi selville. Rikoksentekijän avustaminen peittämisessä tai häivyttämisessä voi tarkoittaa omaisuuden todellisen luonteen, alkuperän, sijainnin tai siihen kohdistuvien määräystoimien tai oikeuksien peittämistä tai häivyttämistä. Avustaminen voisi tapahtua esimerkiksi perustamalla eri yrityksiä

---

[64] HE 53/2002 vp, 19–20.
[65] HE 53/2002 vp, 36–37.
[66] Ks. Heikkilä 2023, 36. Bulvaanilla tarkoitetaan henkilöä, jota hyödynnetään välikätenä erilaisissa oikeustoimissa, esimerkiksi valejohtajana yrityksessä. Valejohtajaa voitaisiin tarvita esimerkiksi silloin, kun todellisella valtaa käyttävällä vastuuhenkilöllä ei ole liiketoiminnan harjoitukseen vaadittavaa laillista oikeutta.

veroparatiiseihin[67]. Huomattavaa kuitenkin on, että 32 luvun 11 §:n mukaan esirikoksen tekijää ei voida tuomita rahanpesusta. Rahanpesusta tuomitaan siis se, joka syyllistyy 6 §:n 1 momentin 1 kohdassa tarkoitettuun hyödyn tai omaisuuden muuntamiseen tai siirtämiseen peittääkseen tai häivyttääkseen hyödyn tai omaisuuden laittoman alkuperän tai avustaakseen toista rikoksentekijää välttämään rikoksen oikeudelliset seuraamukset tai 2 kohdassa tarkoitettuun peittämiseen tai häivyttämiseen tai mainitun teon yritykseen. Kyseisen luvun säännöksiä ei myöskään sovelleta siihen henkilöön, joka asuu rikoksentekijän kanssa samassa taloudessa ja käyttää tai kuluttaa rikoksentekijän hankkimaa omaisuutta, joka on tarkoitettu yhteistalouden tavanomaisiin tarpeisiin.[68]

Kansainvälisen sääntelyn ja kriminalisoinnin tarkoituksena rahanpesun osalta on ollut yhtenäistää lainsäädäntöä, torjua rahanpesun mittavia, maailmanlaajuisia haittavaikutuksia, kitkeä rahanpesuun liittyvä esirikollisuus, estää rikoshyödyn pääsy osaksi laillista talousjärjestelmää sekä rajoittaa rikollisten hyötymistä rikoksilla ansaitsemistaan tuloista ja varallisuudesta. Rikoshyödyn pääsy osaksi muuta talousjärjestelmää ja rikollisten hyötyminen tuloistaan ja varallisuudestaan on pyritty estämään rikosoikeudellisilla menettämisseuraamuksilla, eli konfiskaatiolla.[69] Kätkemis- ja rahanpesurikosten menettämisseuraamuksista säädetään rikoslain (39/1889) 32 luvun 12 §:n 1 momentissa siten, että omaisuus, joka on ollut 6, 7 tai 9 §:ssä tarkoitetun rikoksen kohteena, on tuomittava valtiolle menetetyksi. Samaisen luvun 12 §:n 3 momentin mukaan estämättä, mitä 1 momentissa säädetään, rahanpesun kohteena ollut omaisuus voidaan valtiolle menetetyksi tuomitsemisen asemesta tuomita esirikoksella loukatulle vahingonkorvauksena tai edunpalautuksena, jos omaisuus on laadultaan tähän sopivaa eikä vahingonkorvausta tai edunpalautusta hänelle ole suoritettu. Menettämisseuraamus on yksi keino rahanpesurikoksia ja järjestäytynyttä rikollisuutta vastaan ja sillä on mielletty olevan mahdollista ja tehokastakin ennaltaehkäisevää vaikutusta niin esirikoksiin kuin rahanpesuunkin. Jos esimerkiksi esirikoksesta seuraava tuomio olisi vähäinen, voi taloudellinen tai materialistinen menetys taas olla merkittäväkin. Kriminalisointi ja menettämisseuraamus vaikuttavat osaltaan myös niihin, joilla ei ole ollut osallisuutta esirikokseen. Menettämisseuraamuksella on tyypillisesti tehostettu rangaistussäännöksiä, sillä rikoksesta ei ole taloudellista eikä materialistista hyötyä menettämisseuraamuksen vuoksi. Kuitenkin viimeaikaisten arvioiden mukaan rikollisverkostojen hallusta takaisin peritty rahamäärä on ainoastaan yhdestä kahteen prosenttia järjestäytyneen rikollisuuden vuosituotoista.[70]

---

[67] Ks. Verohallinto 2024. Veroparatiiseilla viitataan maihin, joita hyödynnetään usein veronkierrossa, sillä tällaisissa maissa pankkisalaisuuden taso on kireä ja verotustaso matala. Veroparatiisimaissa ei usein ole kansainvälistä lainsäädäntöä tai sopimuksia omistajuuksien ja verotuksen suhteen.
[68] HE 53/2002 vp, 36–37.
[69] Sahavirta 2008, 5–8.
[70] Sahavirta 2008, 8. Ks. myös Europol 2024a, 4. Samansuuntaista arviota esittää myös FATF 2024, 5.

Rikoshyödyn pääsy osaksi laillista talousjärjestelmää tapahtuu suuressa mittakaavassa usein eri palveluntarjoajien kautta. Talousrikolliset perustavat usein erilaisia kompleksisia yrityksiä ja organisaatioita tai hyödyntävät asiantuntijaverkostojaan esimerkiksi rahoitus- ja kiinteistöalalla rikosten tekemiseksi.[71] Toisaalta tunnettu englanninkielinen talousrikollisuuden termi ”white collar crime”, joka synnyttää mielikuvan varakkaista, suurista ja kansainvälisistä toimijoista, ei aina kuvaa rahanpesun todellisuutta. Esimerkiksi tietyn henkilön ystävän varastaman polkupyörän kauppaaminen eteenpäin voidaan lain silmissä tulkita rahanpesuksi. On siis syytä muistaa, että rahanpesu on ilmiönä moniulotteinen ja rikollinen toiminta on usein moitittavuudeltaan hyvinkin kirjavaa.[72]

4.1 Rahanpesun mekanismit

Rahanpesu on tiettävästi yhteydessä järjestäytyneeseen rikollisuuteen, kuten ihmiskauppaan, erilaisiin petoksiin, veronkiertoon, huumausainerikollisuuteen ja muuhun salakuljetukseen, tavaroiden väärentämiseen, laittomaan asekauppaan ja harvinaisten eläinten salakuljettamiseen.[73] Koska järjestäytyneen rikollisuuden tuotot ovat päätähuimaavia, on ilmiselvää, että osaa tuotoista tarvitaan suuren mittakaavan toiminnan jatkamiseen. Osa rahoista taas menee muihin tarkoituksiin rahanpesun avulla, sillä rikollisesta toiminnasta ei ole mitään hyötyä, mikäli varoja ei päästä käyttämään. Rikollisorganisaatioiden toiminta on pitkälle kehittynyttä, kansainvälistä ja usein hyvin monimutkaista, ja kasvava trendi talousrikollisuudessa on ollut samansuuntainen. Tällaisilla suurilla organisaatioilla on myös syvät yhteydet muihin laillisiin toimiin ja korruptioon. Esimerkiksi suuret huumekartellit ja Italian mafia ovat hyviä esimerkkejä pitkälle edenneestä järjestäytyneestä rikollisuudesta: tällaiset järjestöt hyödyntävät omia asianajajiaan, kirjanpitäjiään ja muita ammattilaisverkostojaan osana toimintaansa. Euroopan Unionin alueella toimivista rikollisjärjestöistä n. 70 % hyödyntää rahanpesua toimintansa jatkamisessa ja varojen alkuperän häivyttämisessä, ja samaisista järjestöistä 60 % hyödyntää korruptiota rikollisen toimintansa mahdollistajana.[74]

Euroopan alueen yhtenäisyys, avoimet hyödykemarkkinat, ihmisten ja varallisuuden vapaa liikkuvuus ovat sekä rikollisuuden mahdollistamisen kuin myös rikollisuuden torjunnan merkittäviä osatekijöitä.[75] Myös lisääntynyt läsnäolo verkossa niin ihmisten kuin yrityksienkin osalta on yksi vaikuttava tekijä järjestäytyneen rikollisuuden ja sitä kautta myös talousrikollisuuden sijoittumiseen EU:n alueelle. Talousrikokset koskettavat kuitenkin myös muuta maailmaa,

---

[71] Europol 2024a, 2.
[72] Heikkilä 2022, 5.
[73] Sahavirta 2008, 20; FATF 2024. Ks. myös Savona & Manzoni 2013, 5.
[74] Savona & Manzoni 2013, 4–5; Europol 2024a, 3–4.
[75] Savona & Manzoni 2013, 2.

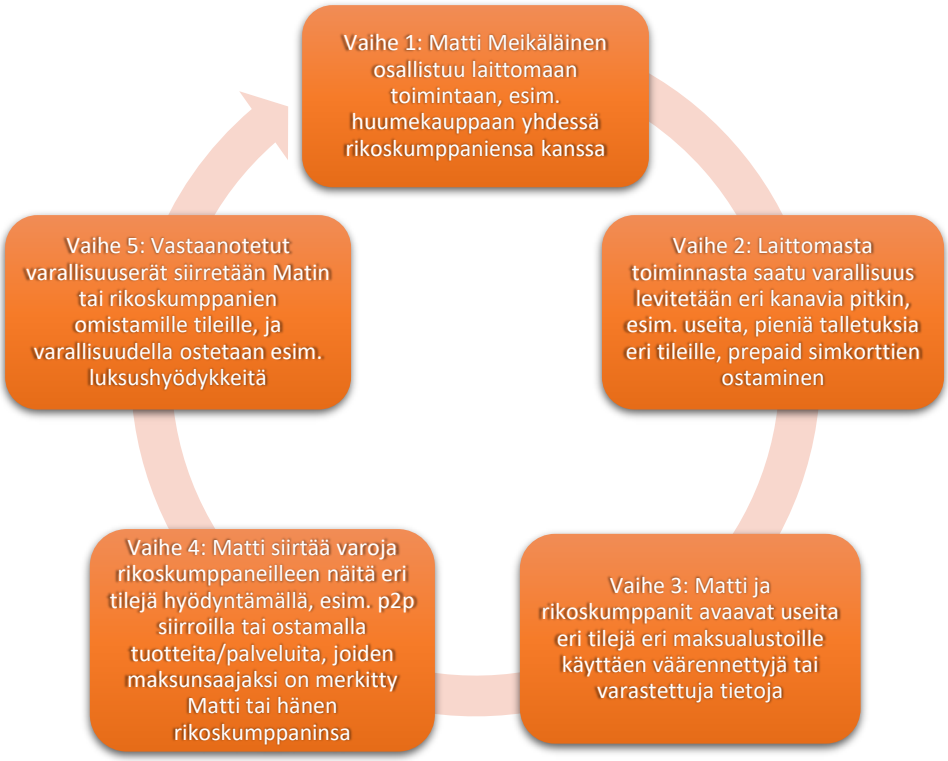
mutta vahvan taloustilanteen ja korkean elintason vuoksi EU:n alue on otollinen paikka talousrikollisuudelle, sillä toimintaa ohjataan usein EU-alueen ulkopuolelta. Toimiminen ns. offshore alueilla[76] ja muilla lainkäyttöalueilla on rikollisilta usein tietoinen päätös, sillä tällaisilla alueilla lainvalvontayhteistyössä sekä kansainvälisten normien ja lakien noudattamisessa on hyvin usein rikollisia hyödyttäviä puutteita. Lisäksi eri alueilla sijaitsevien monimutkaisten yritysrakenteiden avulla tosiasiallisten hyötyjien piilottaminen on helpompaa.[77] Rahanpesu on rikollisuuden muotona kehittynyt muuta rikollisuutta merkittävämmin organisaatiomaiseen, järjestäytyneeseen muotoon, ja tämä voidaan nähdä modernien yhteiskuntien kehityksen varjopuolena. Toisin sanoen, rikollisjärjestöjen monimutkaisuus ja kehittyneisyys peilaa suoraan modernien taloudellisten ja sosiaalisten tekijöiden kehittyneisyyteen.[78]

Rahanpesuprosessin toteutus riippuu usein pestävästä rahamäärästä, rahanpesuprosessin kustannuksista ja siitä, kuinka nopeasti on tarve saada pestyt varat käyttöön. Mittavan järjestäytyneen rikollisuuden parissa prosessin toteutus vaatii usein eri ammattilaisten yhteistyötä, aikaa sekä rahaa, sillä pestävien varojen suuri määrä tai pestävän tulovirran jatkuvuus edellyttää usein myös monimutkaisempia toimenpiteitä. Rikollisen toiminnan pienemmissä pestävissä tuotoissa toteutuskin on usein vaatimattomampaa.[79] Rahanpesu mielletään yleisesti kolmivaiheiseksi prosessiksi, johon kuuluu sijoitusvaihe (placement), harhautusvaihe (layering) ja palautusvaihe (integration).[80] Nämä vaiheet voivat olla toisistaan erillisiä tai muodostaa tietynlaisen jatkumon likaisen rahan häivyttämisessä osaksi laillista talousjärjestelmää. Kaikissa kolmessa rahanpesun vaiheessa rahanpesijä hyödyntää yhtä tai useampaa menetelmää, erilaisia mekanismeja sekä eri rahavälineitä. Rahanpesun menetelmiin voi kuulua esimerkiksi käteisen rahan siirtäminen paikasta toiseen joko fyysisesti tai pankkisiirron avulla tai taloudellisen hyödyn häivyttäminen osaksi laillisia järjestelmiä. Rahanpesun mekanismeihin voi kuulua taloudelliset tai ei-taloudelliset mekanismit. Taloudellisiin mekanismeihin voi kuulua mm. pankkeja tai muita rahoituslaitoksia, kuten valuutanvaihtajia. Ei-taloudellisiin mekanismeihin voi sisältyä taas minkälaisia yrityksiä hyvänsä, kuten kasinoja. Rahavälineisiin voi kuulua mm. kultaa, eri valuuttoja, pankkivekseleitä ja pankki- tai rahasiirtoja.[81]

Rahanpesuprosessiin mielletään myös sisältyvän kaksi erilaista lähestymistapaa. Ns. ”alemman tason” kaupankäyntiä toteuttavat rikollisryhmät suosivat yleensä rahan nopeaa käyttämistä ja hyödyntävät käteistä rahaa suurimmassa osassa toimintaansa. Tässä suppeammassa tavassa laittomasti ansaittu käteinen raha muunnetaan johonkin kaupankäyntiin kelpaavaan,

[76] Ks. esim. Hampton & Levi 1999, 649. Offshore alueilla viitataan pieniin lainkäyttöalueisiin tai mikrovaltioihin, jotka sijaitsevat useimmiten pienillä saarilla.
[77] Europol 2024a, 2–3.
[78] Savona & Manzoni 2013, 2.
[79] Sahavirta 2008, 24–25.
[80] Savona & Manzoni 2013, 3; Sahavirta 2008, 26; Arman 2023, 39.
[81] Savona & Manzoni 2013, 3.

neuvoteltavissa olevaan välineeseen tai omaisuuserään. Tämänkaltaiset ryhmät ja niiden jäsenet suosivat yleensä käteisen rahan käyttöä elinkustannustensa hoitamiseen sekä rikollisten yhteistyötahojensa kanssa toimimiseen, ja välttelevätkin erilaisia taloudellisia toimijoita. Laajemmassa tavassa prosessi alkaa siitä, mihin rahan muuntaminen johonkin toiseen muotoon päättyy ja sisältää edellä mainitut sijoitus-, harhautus- ja palautusvaiheet.[82] Kuviossa 3 on esitetty esimerkkitapaus rahanpesusta.



Kuvio 3: Kuvitteellinen esimerkki rahanpesuprosessin etenemisestä (mukaillen KPMG 2023, 3)

Kuvion 3 ensimmäisessä vaiheessa on kuvattu esirikoksen tekeminen osana rahanpesuprosessia. Matti ja rikoskumppanit ovat myyneet huumeita taloudellisen hyödyn saavuttamiseksi, jolloin esirikos voisi olla Suomen rikoslain (39/1889) luvun 50 mukaisesti yksityiskohdista riippuen huumausainerikos (pykälä 1) tai törkeä huumausainerikos (pykälä 2). Sijoitusvaiheessa rikollisella toiminnalla, kuten esimerkin mukaisella huumekaupalla, saavutettu taloudellinen rikoshyöty saatetaan osaksi laillista talousjärjestelmää.[83] Tässä tapauksessa eri pankeissa tai rahoituslaitoksissa sijaitseville tileille jokainen rikoskumppani siirtää eri suuruisia summia, ja osa saadusta rikoshyödystä käytetään prepaid sim-korttien ostamiseen. Levittämällä

[82] Savona & Manzoni 2013, 4.
[83] Savona & Manzoni 2013, 3.

talletetut rahat eri pankkeihin ja eri tileille vastaanottajien on vaikeampi havaita, että kaikki varallisuus on tosiasiassa peräisin samasta laittomasta toiminnasta.[84] Rikoshyöty voi siirtyä osaksi laillista talousjärjestelmää myös kulutustavaroiden hankkimisella, joka tässä tapauksessa on prepaid sim-korttien ostamista.[85] Harhautusvaiheessa tarkoituksena on erottaa laillisiin järjestelmiin siirretyt varat niiden laittomasta alkuperästä ja pyrkiä salaamaan niitä käyttävien henkilöllisyydet.[86] Vaiheessa 3 Matti ja hänen rikoskumppaninsa avaavat uusia tilejä eri maksualustoille hyödyntäen varastettuja tai väärennettyjä henkilötietoja salatakseen omat henkilöllisyytensä. Vaiheessa 4 aiemmin eri tileille talletetut pienet rahasummat siirretään jälleen eteenpäin hyödyntämällä näitä uusia tilejä eri maksualustoilla, esimerkiksi p2p siirtojen[87] muodossa. Palautusvaiheessa näennäisesti laillinen alkuperä rahalle on luotu, jolloin raha voidaan sijoittaa julkisesti osaksi laillista talousjärjestelmää.[88] Vaiheessa 5 lailliseksi näyttävältä saatu varallisuus siirretään Matin ja rikoskumppaneiden käyttöön. Pestyllä varallisuudella voidaan ostaa esimerkiksi luksustuotteita. Jokaiseen rahanpesuprosessin siirtymävaiheeseen liittyy riski kiinnijäämisestä.[89] Erityisen riskialtis on sijoitusvaihe (kuviossa 3 vaihe 2), sillä rahanpesijä altistuu laillisen talouden edustajien velvollisuuksille asiakkaidensa tuntemisesta ja epäilyttävien liiketoimien raportoimisesta.[90]

Yhteiskuntien taloudellisen ja sosiaalisen kehityksen lisäksi myös rahoitusteknologian (FinTech) nopea kehitys on ajankohtainen aihe niin turvallisuuden, sääntelyn kuin rahanpesunkin kannalta. Kansainvälisessä sääntelyssä on vielä merkittäviä puutteita liittyen virtuaalimuotoiseen omaisuuteen, varallisuuteen ja tällaisten palveluiden tarjoajiin. Uudet teknologiat ja innovaatiot rahoitusmarkkinoilla lupaavat entistä nopeampia, halvempia ja turvallisempia ratkaisuja maksujenkäsittelyyn, mutta FATF:n raporttien mukaan virtuaalivarallisuuden väärinkäyttö rikollisiin tarkoituksiin, kuten laittomien varojen nopeaan liikuttamiseen ja toiminnan häivyttämiseen, ovat kasvava ongelma maailmanlaajuisesti. Suurin osa lainkäyttöalueista noudattaa FATF:n suosituksia asiakkaiden ja tosiasiallisten omistajien tuntemisesta sekä epäilyttävän liiketoiminnan ilmoittamisesta vain osittain, tai ei ollenkaan.[91] Maksujen ja maksupalveluiden nopeutuminen, kansainvälistyminen ja siirtyminen digitaaliseen muotoon syrjäyttänee perinteisiä pankki- ja maksupalveluita. Vuonna 2022 maailmanlaajuisten, digitaalisten maksujen markkinoiden kooksi arvioitiin 81 miljardia Yhdysvaltain dollaria, ja vuosittaisen

---

[84] Sahavirta 2008, 27 mukaan Galli & Wexton 1996, 362.
[85] Sahavirta 2008, 26.
[86] Sahavirta 2008, 31; Savona & Manzoni 2013, 3.
[87] Ks. Wall Street Journal 2023. P2P (peer-to-peer) maksuilla tarkoitetaan kahden henkilön välisiä rahasiirtoja, joissa ei tarvita fyysistä pankkikorttia tai käteistä. P2P maksumahdollisuutta tarjoavat nykyisin useat eri alustat ja sovellukset, kuten MobilePay.
[88] Savona & Manzoni 2013, 3.
[89] Sahavirta 2008, 34 mukaan Schaap 1998, 14. Sahavirta toteaa Schaapin kuvaavan näitä kiinnijäämisen riskivaiheita termillä ”choke points”.
[90] Sahavirta 2008, 34.
[91] FATF 2024, 6.

markkinoiden kasvun on arvioitu olevan jopa 20 % seuraavan seitsemän vuoden aikana. Kuten aiemmin todettu, yhteiskunnan moderni kehitys peilaa suoraan myös rikollisjärjestöjen kehittyneisyyteen. Rikolliset kehittelevätkin siis aktiivisesti omia digitaalisia maksutuotteita -ja palveluita pysytellen FinTechin nopean kehityksen perässä. FinTechin kehitys voi siis osaltaan kasvattaa myös talousrikollisuuden esiintyvyyttä, yleensä rahanpesun, terrorismin rahoittamisen, sanktioriskin[92] ja petosten muodossa.[93] Erilaiset petokset voivat kohdistua niin yksityishenkilöihin kuin yrityksiinkin. Tyypillisimpiä ovatkin sijoituspetokset (kryptovaluuttoihin liittyvät), yrityssähköpostipetokset, digitaalisen kaupankäynnin petokset, teknisiä tukipalveluita tarjoaviin liittyvät petokset, tietojenkalastelu ja romanssihuijaukset. Erilaisilla tukipetoksilla, tullipetoksilla, arvonlisäveropetoksilla ja valmisteveropetoksilla EU:n alueella on miljardien eurojen hyöty petosten tekijöille vuosittain. Suurin osa petoksista tapahtuu tietoverkkoavusteisesti.[94]

Suomessa rahanpesuun, sen selvittämiseen ja torjuntaan liittyviä tehtäviä hoitaa Keskusrikospoliisin alaisuudessa toimiva Rahanpesun selvittelykeskus.[95] Selvittelykeskuksen toiminnan keskiössä ovat pankkien tekemät ilmoitukset riskiperusteisesta rahanpesusta, toisin sanoen pankit siis ilmoittavat selvittelykeskukselle epäilyttäväksi havaitsemastaan liiketoiminnasta riskiperusteisesti tai summaperusteisesti.[96] Vuoden 2023 aikana selvittelykeskus analysoi selvityksessään, että vähintään neljäsosa selvittelykeskuksen vastaanottamista riskiperusteisista rahanpesuilmoituksista liittyi petoksiin. Samassa selvityksessä havaittiin myös, että merkittävä osa petoksilla saaduista taloudellisista hyödyistä pestiin ulkomailla usein finanssialan toimijoiden välityksellä. Taloudellisen hyödyn saavina osapuolina näissä petostapauksissa esiintyivät yleisimmin liettualaiset, saksalaiset, italialaiset, ranskalaiset sekä espanjalaiset eri finanssialan toimijoiksi rekisteröityneet tahot. Aiemmin mainitun FinTechin kehityksen haittapuolet on huomattu myös selvittelykeskuksessa: vuoden 2023 aikana selvittelykeskuksessa huomattiin FinTech yrityksiin liittyvien vIBAN:ien (virtuaalisten kansainvälisten tilinumeroiden) käytön yleistyneen petosrikollisuudessa.[97] Petoksia ja tietojenkalastelua on käyty läpi myös kappaleissa 3.1 ja 3.2.

[92] Ks. Finanssivalvonta 2022, 6–7. Sanktioriski muodostuu, kun rahoituslaitokset tai muut taloudelliset toimijat laiminlyövät sellaisia toimia joihin laki velvoittaa, esimerkiksi rahanpesun estämisen valvontaa.
[93] KPMG 2023, 1.
[94] Europol 2024a, 4–5.
[95] Poliisi 2024d.
[96] Rahanpesun selvittelykeskus 2023, 27.
[97] Rahanpesun selvittelykeskus 2023, 10–11.

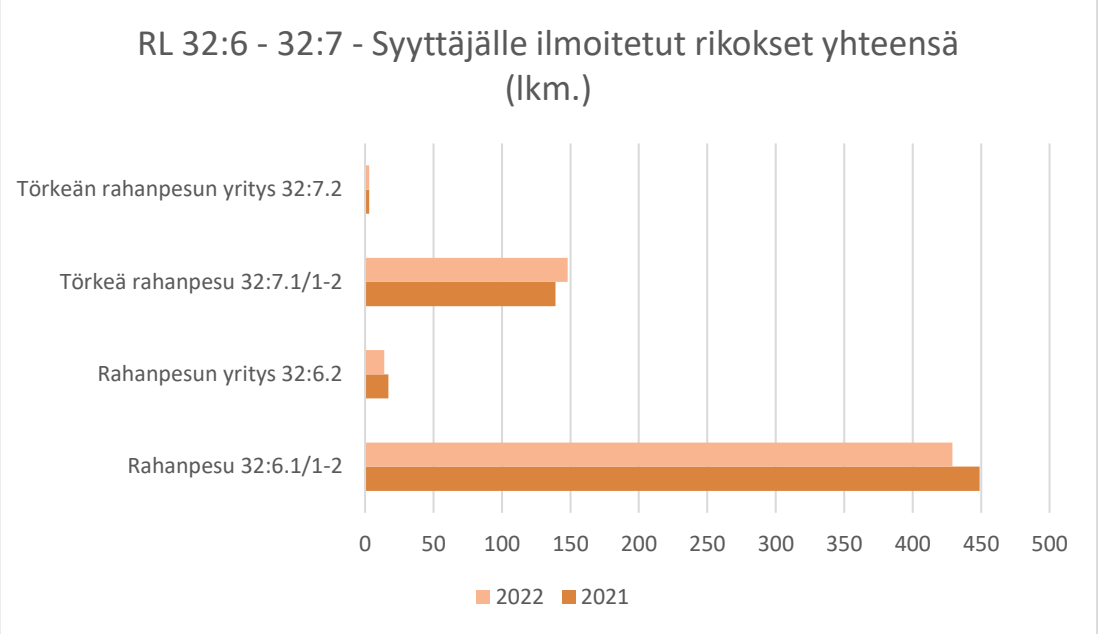
4.2 Rahanpesu osana talousrikollisuutta ja yleisyys Suomessa

Vuonna 2023 pankit ilmoittivat Rahanpesun selvittelykeskukselle yhteensä 19 847 tapausta, ja eroa edeltävään vuoteen 2022 oli 49 prosenttia. Ilmoituksien perusteella on voitu tehdä myös paikallistamista liittyen henkilöihin, yhtiöihin, tilien tosiasiallisiin toimintamaihin sekä lainkäyttöalueisiin liittyen. Vuoden 2023 ilmoituksien perusteella henkilöitä voitiin paikantaa yhteensä 177 eri lainkäyttöalueelle, joista yleisimpiä olivat Suomi, Ukraina ja Venäjä. Yhtiöitä paikallistettiin yhteensä 137 eri lainkäyttöalueelle, joista yleisimpiä olivat Suomi, Saksa ja Viro. Tilejä paikallistettiin yhteensä 145 eri lainkäyttöalueelle, joista yleisimpiä olivat Suomi, Liettua ja Viro. Vastaanotettuihin ilmoituksiin liittyvien varallisuuksien kokonaissummat vuonna 2023 olivat keskimäärin 10 000–49 999 euroa. Saman vuoden aikana selvittelykeskus kirjasi rahanpesurekisteriinsä transaktioita yli 1,9 miljoonaa kappaletta, ja näiden yhteenlaskettu arvo oli noin 2,5 miljardia euroa. 1,9 miljoonan transaktion joukosta 72 000 koski virtuaalivaluuttoja, joiden arvo siirtohetkellä oli noin 212 miljoonaa euroa. Rekisteriin kirjattiin myös erikseen transaktiot, joiden kohde- tai lähtömaa oli Suomi, ja joiden toiset kohde- tai lähtömaat oli pystytty paikallistamaan. Näiden Suomeen kohdennettujen transaktioiden yhteissumma oli 335 990 132 euroa, ja yleisimmin lähtömaina esiintyivät Armenia, Tšekki, Kiina (Hongkong), Viro ja Venäjä. Suomesta ulkomaille kohdennettujen transaktioiden yhteissumma oli 194 949 702 euroa, ja yleisimmin kohdemaina esiintyivät Viro, Kypros, Liettua, Yhdistynyt kuningaskunta ja Sveitsi.[98]

Vuoden 2023 aikana selvittelykeskus avasi 1452 juttua, joista 1192 jutussa tehtiin vähintään yksi tiedonluovutus eteenpäin, näistä 544 jutussa luovutettiin tietoja esitutkintatarkoituksiin ja 29 jutussa luovutettiin tietoja rikosilmoitukseen. Eniten tietoja luovutettiin kotimaisista viranomaisista poliisilaitoksille, Keskusrikospoliisille sekä Verohallintoon. Yleisimmät törkeät rikosnimikkeet, joita varten selvittelykeskuksen tietoja luovutettiin, olivat törkeä petos (19 % tapauksista), törkeä maksuvälinepetos (6 % tapauksista), törkeä huumausainerikos (4 % tapauksista) sekä törkeä rahanpesu (4 % tapauksista). Viime vuosien aikana törkeiden petosten osuus on kasvanut.[99] On kuitenkin syytä muistaa, että rahanpesu tapahtuu osittain yhteiskunnan laillisen puolen ulottumattomissa, jolloin sen laajuuden ja eri määrien luotettava arviointi on mahdotonta. Rahanpesun esiintyvyyttä arvioidaan yleensä osana harmaata taloutta, jonka määrää taas pyritään laskemaan välillisesti makrotalouden indikaattoreiden tai välittömästi tilastojen avulla.[100] Suomessa harmaan talouden osuus bruttokansantuotteesta vaihtelee miljardista eurosta aina 14 miljardiin euroon asti.[101] UNODC:n (United Nations on Drugs and Crime) arvion mukaan 2–5 prosenttia maailmanlaajuisesta bruttokansantuotteesta pestään

[98] Rahanpesun selvittelykeskus 2023, 27–29.
[99] Rahanpesun selvittelykeskus 2023, 29–32.
[100] Sahavirta 2008, 38.
[101] Sisäministeriön sisäisen turvallisuuden sivusto TUOVI 2023.

vuosittain. Summa on siis arviolta 715 miljardin ja 1,87 biljoonan euron väliltä vuosittain.[102] Taulukossa 4 on esitetty Suomessa syyttäjälle ilmoitetut rahanpesurikokset vuosina 2021–2022.



Taulukko 4: Syyttäjälle ilmoitetut rahanpesurikokset vuosina 2021–2022[103]

Törkeitä rahanpesun yrityksiä ilmoitettiin syyttäjälle vuonna 2021 ja 2022 yhteensä vain kolme kappaletta, ja törkeitä rahanpesuja 139 kappaletta vuonna 2021 ja 148 kappaletta vuonna 2022. Rahanpesun yrityksiä ilmoitettiin syyttäjälle vuonna 2021 yhteensä 17 kappaletta ja 2022 14 kappaletta. Taulukosta 4 on nähtävissä, että perusmuotoinen rahanpesu on yleisin toteutettu rikosmuoto. Perusmuotoisia rahanpesuja ilmoitettiin 449 kappaletta vuonna 2021 ja 429 kappaletta vuonna 2022. Määrät ovat pysyneet samansuuntaisina. Rikoslain (39/1889) 32 luvun 6 §:n mukaan rangaistus perusmuotoisesta rahanpesusta on sakkoa tai enintään kaksi vuotta vankeutta, ja 7 §:n mukaan rangaistus törkeästä rahanpesusta on vähintään neljä kuukautta ja enintään kuusi vuotta vankeutta. Esimerkiksi KKO 2020:98 ennakkopäätöksessä rikoksentekijä A:n syyksi luettu rangaistus avunannosta törkeään velallisen epärehellisyyteen, törkeästä rahanpesusta ja kolmesta rekisterimerkintärikoksesta oli 1 vuotta ja 3 kuukautta ehdollista vankeutta, yhdyskuntapalvelua 30 tuntia sekä neljän vuoden liiketoimintakielto. Korkeimman oikeuden ennakkopäätöksessä KKO 2019:110 rikoksentekijä A:n syyksi luettiin törkeä rahanpesu, rattijuopumus ja ampuma-aserikos, josta rangaistus oli yhdeksän kuukautta ehdollista vankeutta. Ennakkopäätöksessä KKO 2009:59 rikoksentekijä S:n syyksi

[102] Europol 2024b.
[103] Tiedot StatFinista.

luettiin rahanpesu. Korkein oikeus pitäytyi hovioikeuden antamassa tuomiossa, joka oli 80 päiväsakkoa.

Suomessa talous- ja huumausainerikollisuuden tuotot ovat arvioitu olevan yleisin rahanpesemisen kohde, ja tavallisimpia talousrikoksia Suomessa ovat verorikokset ja velallisen rikokset. Rahanpesun yleisyyden määrä Suomessa on yleensä suurempi kuin annettujen rahanpesutuomioiden määrä. Selittävänä tekijänä on arvioitu olevan rangaistuksettomat jälkiteot, eli sellaiset toimet, jotka rikoksentekijä kohdistaa omilla rikoksillaan saatuun omaisuuteen. Tällaiset teot katsotaan Suomessa rangaistuksettomiksi jälkiteoiksi. Suomessa talousrikostutkinta on tehokasta ja talousrikoksista syntynyt vahinko on usein suurempi kuin esimerkiksi huumausainerikollisuudesta saatu tuotto. Myös näillä seikoilla on arvioitu olevan vaikutusta rahanpesurikosten yleisyyteen Suomessa.[104]

Vuoden 2021 erityiskertomuksessaan Euroopan tilintarkastustuomioistuin havaitsi, että rahanpesun ja terrorismin rahoituksen torjumisessa on puutteita unionitasolla. Tilintarkastustuomioistuin kuvaili rahanpesun ja terrorismin rahoituksen estämisessä ja riskeihin puuttumisessa olevan institutionaalisia hajanaisuuksia ja koordinoinnin ongelmia. Lisäksi tuomioistuin huomautti, ettei unionin alueella ole yhteistä rahanpesun ja terrorismin rahoituksen valvojaa, jolloin toimivalta on jaettua ja koordinointi jäsenvaltioiden kanssa siten myös erillistä.[105] Heinäkuussa 2021 Euroopan unionin komissio teki ehdotuksen lainsäädäntöpaketista, jonka tarkoituksena oli tehostaa EU:n rahanpesun ja terrorismin rahoittamisen torjuntaa koskevia sääntöjä sekä parantaa niiden valvomista. Helmikuussa 2024 neuvosto ja parlamentti saavuttivat alustavan sopimuksen rahanpesun torjuntaan liittyvien paketin osista. Lakipakettiehdotukseen kuului mm. rahanpesun vastaisten mekanismien direktiivi (COM/2021/423), joka myös osaltaan kumoaisi direktiivin rahoitusjärjestelmän käytön estämisestä rahanpesuun tai terrorismin rahoitukseen (EU) 2015/849. Lisäksi ehdotukseen sisältyi asetus (COM/2021/421), jossa ehdotettiin perustettavaksi uusi rahanpesuntorjuntaviranomainen AMLA (Anti-Money Laundering Authority).[106] AMLA:n uudeksi kotipaikaksi on valittu Frankfurt, ja se aloittaa toimintansa vuonna 2025.[107] Ehdotukseen sisältyi myös asetus rahanpesunvastaisista velvoitteista (COM/2021/420), joita sovellettaisiin yksityiseen sektoriin. Lisäksi ehdotukseen kuului asetus varainsiirtoja koskevan asetuksen uudelleenlaatimisesta (COM/2021/422), jonka tarkoituksena on tehdä kryptovarojen siirtämisestä jäljitettävää ja avointa sekä tehdä muutoksia direktiiviin (EU) 2015/849.[108] Komission ehdotuksesta muodostunutta säädöstä (EU/2023/1113) aletaan soveltamaan jäsenvaltioissa joulukuussa 2024.[109] Niin kutsuttu EU:n AML-paketti kattaa siis

[104] Sahavirta 2008, 40 & 42.
[105] Euroopan tilintarkastustuomioistuin 2021, 48.
[106] Euroopan unionin neuvosto 2024a, 3.
[107] Euroopan unionin neuvosto 2024b, 1.
[108] Euroopan unionin neuvosto 2024a, 3.
[109] Euroopan unionin virallinen lehti (EUVL) L 150 2023, 36.

neljä sääntelykokonaisuutta: AMLA:n perustamisen, rahanpesun ja terrorismin rahoittamisen torjuntaa koskevan asetuksen, kuudennen rahanpesun ja terrorismin rahoittamisen torjuntaa koskevan direktiivin sekä asetuksen kryptovarojen siirtojen tehokkaammaksi jäljittämiseksi. Lakipaketin neuvottelujen on arvioitu olevan valmiita keväällä 2024.[110]

5 Turvallisuus finanssialalla

Petos -ja talousrikollisuuden määrä sekä niistä aiheutuvat kustannukset ovat kasvaneet merkittävästi. Vuonna 2018 WEF (World Economic Forum) arvioi petos -ja talousrikollisuuden olevan jopa biljoonan dollarin arvoinen ala ja yksityisten yritysten arvioitiin käyttäneen jopa 8,2 miljardia dollaria rahanpesun vastaisiin toimiin vuonna 2017. Lisäksi eri toimijoiden arvioitiin menettävän kolme dollaria jokaista petoksessa menetettyä dollaria kohtaan, kun petoksesta johtuvaan tappioon on laskettu mukaan muut siihen liittyvät kustannukset. Pankkeihin kohdistuvat turvallisuusriskit koostuvat monesta eri tekijästä. Maksutapahtumien kasvanut määrä, pankkitoiminnan siirtyminen eri maiden välille ja verkkoon aiheuttavat riskejä pankkien turvallisuudelle. Lisäksi automaation ja digitalisaation haavoittuvuudet lisäävät petoksien ja muun talousrikollisuuden riskejä luottolaitoksissa. Eri kyberrikollisuuden muodot ja hakkerointi ovat myös kasvava ongelma pankkialan turvallisuudelle. Rahoitusalan digitalisaation ja automatisoinnin vuoksi myös rikoksista on tullut elektronisesti monimutkaisempia.[111] Myös Suomessa on todettu tietoverkkoavusteisen petosrikollisuuden vakiintunut asema. Esimerkiksi poliisihallinnossa on jatkossa erillinen yksikkö, joka tutkii ja selvittää laajempia tietoverkkoavusteisia petoskokonaisuuksia, sillä petosrikollisuuden taustalla on usein suurempia petoskokonaisuuksia ja järjestäytynyttä rikollisuutta.[112]

Yleensä eri rahoitusalan toimijat tekevät rajanvetoa petoksien ja talousrikollisuuden välille, jotta niitä olisi helpompi ehkäistä ja tunnistaa. Talousrikollisuuteen on yleensä laskettu kuuluvaksi rahoitusalan toimijoiden näkökulmasta esimerkiksi rahanpesu, lahjonta ja veronkierto. Nämä seikat on yleensä nähty osana yritysten lainsäädännön, määräysten ja eettisten periaatteiden noudattamista. Petosrikollisuuteen taas on luokiteltu kuuluvan esimerkiksi väärennökset, luottopetokset ja sisäiset uhat, jotka useimmiten liittyvät henkilöstön harhauttamiseen rikosten tekemiseksi. Rajanveto ei ole peräisin finanssialan regulaatiosta tai muustakaan lainsäädännöstä, ja erilaisten rahoitusalan toimijoiden kohtaamien kyberuhkien vuoksi rajanveto on häilyvää.[113] Toisaalta siis kyberuhkien, petoksien ja esimerkiksi rahanpesun taustalla on

[110] Rahanpesun selvittelykeskus 2023, 36.
[111] Hasham, Joshi & Mikkelsen 2019, 2. Samansuuntaisesti talousrikollisuuden kehityksen peilaavuudesta yhteiskuntien teknologian kehitykseen ovat todenneet myös Savona & Manzoni 2013, 2.
[112] Rahanpesun selvittelykeskus 2023, 2 & 35.
[113] Hasham, Joshi & Mikkelsen 2019, 2.

usein samanlaisia, yhdistäviä tekijöitä, kuten järjestäytynyttä rikollisuutta, tietoverkkosidonnaisuutta -ja avusteisuutta. Esimerkiksi järjestäytyneen rikollisryhmän suorittama hakkerointi voi edellyttää tietojenkalastelun tai petoksen tekemistä, ja petoksilla sekä hakkeroinnilla saadut varallisuudet taas rahanpesua. Yhdistävien taustatekijöiden ja piirteiden vuoksi rahoitusalan toimijoiden olisi tärkeä tunnistaa näiden seikkojen verkottuminen ja yhdistyminen toisiinsa, jotta ennaltaehkäisy ja puuttuminen niihin olisi tehokkaampaa. Järjestäytyneen rikollisuuden määrittely on myös olennainen seikka rikollisuuden ja turvallisuuden kontekstissa. Järjestäytynyttä rikollisuutta terminä voidaan määritellä kolmen piirteen perusteella:

1. Rikoksiin syyllistyvä organisaatio koostuu joukosta ihmisiä, jotka tekevät yhteistyötä pitkään tai määrittelemättömän ajan.
2. Väkivaltaa tai sen uhkaa hyödynnetään kurin ylläpitämisessä, uhkien tai kilpailijoiden poistamisessa tai pelottelussa. Korruptiota hyödynnetään erillisenä tekijänä tai väkivallan yhteydessä mahdollisuuksien kasvattamiseksi, käyttämällä esimerkiksi poliitikkoja juonittelun keinona julkisten sopimuksien saamiseksi. Korruptio ei aina liity suoraan taloudelliseen hyötymiseen, vaan se voi olla myös palvelusten vaihtoa eri toimijoiden kesken.
3. Hierarkkinen tai joustava organisaatiomainen rakenne, joka muuttuu organisaation tehtävien mukana. Nämä tehtävät vaativat usein tiedonsaantia ja viestintää.

Järjestäytyneen rikollisuuden perimmäinen tarkoitus on mahdollisimman suuri voitto, ja sitä varten organisaatio tarvitsee vaikutusvaltaa ja voimaa, jota ryhmässä toimiminen yleensä tuo.[114] Nykypäivän talousrikosten ja petosten kyberprofiilia sekä näiden taustalla olevaa järjestäytynyttä rikollisuutta havainnollistaa hyvin vuonna 2013 alkaneet Carbanak-hyökkäykset. Carbanak-hyökkäys on havainnollistettu kuviossa 4.

[114] Savona & Manzoni 2013, 2.

Kuvio 4: Carbanak-hyökkäys havainnollistettuna (mukaillen Hasham, Joshi & Mikkelsen 2019, 3)

Carbanak-hyökkäys kohdistettiin useaan eri pankkiin samanaikaisesti. Hyökkäyksen takana ollut järjestäytynyt rikollisryhmä sai pääsyn järjestelmiin tietojenkalastelun avulla. Rikollisryhmä siirsi valheellisesti paisutettuja summia omille tileilleen ja ohjelmoivat pankkiautomaatit antamaan käteistä rikoksessa avustaville. Ensimmäisessä vaiheessa kohdeyrityksen työntekijä joutui kohdennetun tietojenkalastelun uhriksi vastaanottaen sähköpostin, jossa oli liitetiedosto. Toisessa vaiheessa avattuaan liitetiedoston työntekijä aktivoi tietämättään niin kutsutun takaportin, eli pääsyn kohdetietoihin. Kolmannessa vaiheessa haittaohjelma tutki verkkoa ja löysi pääkäyttäjän tietokoneen. Neljännessä vaiheessa pääkäyttäjän tietokone on tunnistettu ja näyttö kaapataan. Hyökkääjä katseli pääkäyttäjän näyttöä etänä matkiakseen pääkäyttäjän toimintaa rahojen siirrossa. Viidennessä vaiheessa hyökkääjä muunsi tilien saldoja todellista suuremmiksi. Kuudennessa vaiheessa hyökkääjät ohjelmoivat pankkiautomaatin antamaan käteistä tiettyinä aikoina automaattien luona odotteleville avustajille. Viimeisessä vaiheessa hyökkääjät hyödynsivät verkkomaksuja siirtääkseen nostetut varat vastaanottaviin pankkeihin.[115]

Carbanak-hyökkäys osoittaa sen, mitä aiemminkin on jo todettu: rikollisten osaaminen kyberympäristössä on kehittynyttä, ja eri osa-alueet järjestäytyneen rikollisuuden maailmassa aina tietojenkalastelusta kyberhyökkäyksiin ja rahanpesuun sekä avustaviin tehtäviin tapahtuvat usein saman järjestön toimesta. Kyberhyökkäykset, petokset ja talousrikokset eivät siis ole enää yksittäisiä toimia, jotka aiheuttavat rahoitusalan toimijoille riskejä, vaan ne muodostavat kasvavan ja kehittyneen kokonaisuuden. Carbanak-hyökkäyksessä tekijät ovat myös ymmärtäneet pankkitoiminnan prosesseja, valvontaa ja haavoittuvaisuuksia, joiden ajatellaan

[115] Hasham, Joshi & Mikkelsen 2019, 3.

johtuvan organisaatioiden ja hallinnon siiloutumisesta. Tämä osoittaa, että rahoitusalan toimijoiden toimintamalleja olisi syytä tarkastella uudelleen.[116]

Erilaiset palvelunestohyökkäykset ovat myös lisääntyneet ja niitä on kohdistettu niin julkisen kuin yksityisenkin puolen toimijoihin ja yrityksiin. Palvelunestohyökkäyksien lisäksi muita kyberuhkia ovat aiemmin mainitut tietojenkalastelu, tietomurrot sekä haittaohjelmat. Finanssivalvonta vastaanottaa rahoitusalan toimijoilta ilmoituksia erilaisista häiriöistä päivittäin. Osa ilmoitetuista häiriöistä liittyy juurikin palvelunestohyökkäyksiin ja kyberrikollisuuteen. Vaikka rahoitusalan toimijat ovat pystyneet varautumaan ja torjumaan erilaisia uhkia tehokkaasti, viranomaisten välistä yhteistyötä ja tiedonvaihtoa on vahvistettu entisestään. Oleellista erilaisten kyberuhkien, kuten petostenkin, ehkäisemisessä on myös palveluiden käyttäjällä itsellään. Eri palveluihin kirjautuessa tulisi käyttää vain virallisia sivustoja ja harjaantua huomaamaan, milloin on esimerkiksi tietojenkalastelusivustolla. Keskiöön nouseekin kansalaisten tietoisuuden ja tarkkaavaisuuden lisääminen aiheista. Internetiä käyttäessä tulisi olla sopivasti epäluuloinen, hyödyntää tietoturvaohjelmistoja sekä varmistaa, että tietokoneessa ja puhelimessa on aina uusin ohjelmistopäivitys asennettuna.[117]

Niin kutsuttu digitaalinen luottamus onkin noussut finanssimaailmassa erottautumistekijäksi asiakaskokemuksessa, sillä yhä enemmän asiakkaat asioivat pankin kanssa virtuaalisesti. Etulyöntiaseman ja positiivisen vaikutuksen kassavirtaan saavat siis ne pankit, joiden digitaalinen käyttöliittymä tekee asiakaskokemuksesta saumattoman, nopean ja turvallisen. Huonoimmassa mahdollisessa skenaariossa näihin seikkoihin varautumatta jättäminen johtaa mainehaittaan, asiakkaiden ja tulojen menettämiseen ja sääntelyn noudattamatta jättämisen haittoihin, kuten seuraamusmaksuihin tai sakkoihin sekä talousrikosten ja petosrikosten kustannuksiin. Tähän skenaarioon ajaa myös toisaalta pankkien keskittyminen vastuiden ja kustannusten vähentämiseen.[118]

Rahoitusalan toimintaa ja sen turvallisuutta ohjaa pitkälti kansainvälinen sääntely. Eräässä vuonna 2008 tehdyssä tutkimuksessa analysoitiin rahoitussektorin sääntelyn ja valvonnan laatua maailmanlaajuisesti. Tutkimuksessa hyödynnettiin IMF:n (International Monetary Fund) ja Maailmanpankin tietoja arvioinneista kansainvälisten standardien noudattamisesta. Rahoitussektorin arviointiohjelmaan (FSAP) kuului tutkimushetkellä noin kaksi kolmasosaa IMF:n 185 jäsenmaasta. Tutkimuksessa havaittiin, että sääntely- ja valvontakehysten laadussa on huomattavia eroja maiden välillä, ja tulojen taso oli myös merkittävä tekijä.[119] IMF:ään kuuluu nykyisin 190 maata ja sen tehtävänä on edistää maailmanlaajuista rahapolitiikan yhteistyötä,

[116] Hasham, Joshi & Mikkelsen 2019, 3.
[117] Koponen 2023. Ks. myös Tanttari & Alanko 2017, 17.
[118] Hasham, Joshi & Mikkelsen 2019, 4.
[119] Čihák & Tieman 2008, 4–5.

turvata taloudellista vakautta, helpottaa kansainvälistä kauppaa, edistää korkeaa työllisyyttä ja kestävää talouskasvua sekä vähentää köyhyyttä maailmanlaajuisesti.[120]

Sekä pankki- että vakuutusvalvonnassa sääntelyn kokonaisnoudattavuuden keskimääräinen taso oli selvityksessä 67 prosenttia. Tämä arvo vastasi kolmatta pistettä käytetyssä neljän pisteen asteikossa, jolloin voitiin todeta, että sääntelyjärjestelmiä noudatettiin pääosin. Sääntelyn ja regulaation noudattamiseen vaikutti myös tarkastellun maan tulotaso. Tutkimuksessa huomattiin, että taloudellisesti vauraampien maiden sääntelyn noudattavuuden taso oli korkeampi kuin köyhempien maiden. Toisaalta suurin ero noudattavuudessa riippuen maan tulotasosta oli korkean tuloluokan ja keskituloluokan välillä. Keskituloisen ja matalamman tuloluokan välinen ero noudattavuuden suhteen oli pienempi. Huomattavia alueellisia eroja havaittiin myös valvonnan laadun suhteen. Euroopan alueella sijaitsevat tarkastellut IMF:n jäsenmaat osoittivat keskimäärin korkeampaa noudattavuustasoa valvonnan suhteen kuin muut alueet. Vielä huomattavampi ero noudattavuuden suhteen oli Euroopan Unioniin kuuluvien maiden ja siihen kuulumattomien eurooppalaisten valtioiden välillä. Vaikka Euroopan alue ja EU:n jäsenmaat osoittivat selvityksessä korkeampaa sääntelyn ja regulaation noudattamisen tasoa, niin pankkitoiminnassa ainoastaan kaksi EU-maata noudatti kaikkia ydinperiaatteita. Yhtäkään periaatetta ei kuitenkaan noudatettu täysin kattavasti edes EU:n alueella. Jokaista noudatettavaa periaatetta kohden oli noin yhdeksän maata, jotka eivät noudattaneet periaatteita täysin. Joidenkin noudatettavien periaatteiden kohdalla jopa yli puolet EU-maista eivät noudattaneet periaatteita täysin.[121]

5.1 Turvallisuuden parantaminen

Finanssivalvonta teki pankeille selvityskyselyn loppuvuodesta 2023. Selvityksessä tuli ilmi, että pankit ovat huolehtineet verkkomaksamisen turvallisuudesta pääosin hyvin. Turvallisuusratkaisujen päivittämisestä on kuitenkin huolehdittava jatkuvasti rikollisuuden kehittyessä. Nykyisellään pankkien keinoina verkkomaksamisen turvallisuuteen ovat erilaiset maarajaukset, verkkomaksurajaukset sekä summaperusteiset turvarajat. Finanssivalvonta suositteli kuitenkin, että pankit kehittäisivät turvatoimintojaan koskemaan laajemmin ja monipuolisemmin mobiili- tai verkkopankin kautta tehtäviä tilisiirtomaksuja. Lisäksi suositeltuna kehitystoimena mainittiin maksujen monitoroinnin tehostaminen, jotta poikkeavien maksujen pysäyttäminen olisi tehokkaampaa. Pankkien on myös tärkeää tiedottaa asiakkaille erilaisista huijaustavoista ja opastaa turvalliseen verkkoasiointiin. Asiakkaiden on oltava tietoisia omasta vastuustaan verkko- ja mobiilimaksamisessa ja vältettävä epäilyttäviä tilanteita, kuten pankkitunnusten

[120] IMF 2022.
[121] Čihák & Tieman 2008, 8–12.

antamista viesteissä olevien linkkien kautta. EU:ssa kehitetään parhaillaan digitaalisen identiteetin lompakkosovellusta, joka tarjoaa uusia tapoja digitaalisen todentamisen helpottamiseen verkkoasiointia varten. Tällaiset välineet voivat osaltaan lisätä turvallisuutta ja vähentää riskejä.[122]

Pankkien muokatessa toimintaansa vastaamaan rikollisuuden muuttuvaan profiiliin, ne pakostikin kohtaavat muun talousrikollisuuden ja petoksien yhteyden kyberrikoksiin. Pankkien menetelmät petosten hallitsemista varten ovat yleensä suoraviivaisia, kanavakohtaisia ja eri pisteytyksiin perustuvia toimenpiteitä. Rahoitusalan johtavien toimijoiden keskuudessa on jo pyritty yhdistämään talousrikosten, petosrikollisuuden ja kyberrikollisuuden ulottuvuudet. Turvallisuuden varmistamisessa ja rahanpesun torjunnassa talousrikosten, petosten ja kyberrikollisuuden integraatio yhteneväisemmäksi kokonaisuudeksi on oleellista kokonaisvaltaisen ennaltaehkäisyn ja turvallisuuden kannalta. Näiden aiheiden integrointi kokonaisuudeksi hankkeena edellyttää pankeilta riskienhallintatoimien tarkkaa määrittelyä sekä roolien ja vastuiden selventämistä. Kiinnittämällä huomiota näihin seikkoihin pankit voivat varmistaa kattavasti ja selkeästi määritellyt toiminnot riskien hallitsemiseksi välttäen turhaa toistoa eri prosessien välillä. Kaikkiin talousrikollisuuden riskeihin sisältyvät vastatoimenpiteet asiakkaan tunnistamisesta ja todentamisesta, transaktioiden ja käyttäytymismallien seurannasta ja havaitsemisesta sekä riskien ja ongelmien lieventämisestä finanssialalla nojautuvat samankaltaisiin prosesseihin ja datan hyödyntämiseen. Näiden tietolähteiden yhdistäminen analytiikkaan mahdollistaisi ennaltaehkäisevät toimet ja tehokkaamman havainnoinnin.[123]

Rahoitusalan kohtaaman talousrikollisuuden eri osien integrointia, eli yhdistämistä tai sisällyttämistä hankkeena voidaan kuvata kolmen erilaisen mallin perusteella. Mallit eroavat toisistaan siinä, kuinka paljon integrointia erilaisiin rikostyyppeihin sisältyvien prosessien ja toimintojen piirissä on. Toimintamallia kehittäessä organisaation ja hallinnon suunnittelu on keskeisessä asemassa. Mallista riippumatta organisaatiossa on onnistuttava tuomaan oikeat ihmiset yhteen, rakentamaan ketteriä tiimejä, kiinnittämään huomiota kokonaisvaltaiseen lähestymistapaan sekä panostamaan teknologiaan ja analytiikkaan. Monet pankkialan toimijat ovat asettaneet tavoitetilakseen osittaisen integraation mallin, pyrkien kuitenkin kokonaan integroituun malliin.[124] Mallit on esitetty taulukossa 5.

[122] Finanssivalvonta 2024b.
[123] Hasham, Joshi & Mikkelsen 2019, 3–5.
[124] Hasham, Joshi & Mikkelsen 2019, 5.

Malli →	**Yhteistyötä korostava malli**	**Osittain integroitu malli**	**Kokonaan integroitu malli**
Kuvaus ↓	Itsenäinen raportointi, roolit ja vastuu jokaiselle rikostyypille	Jokainen talousrikollisuuden yksikkö säilyttää itsenäisyytensä	Yhteisen viitekehyksen alla oleva yhdistetty yksikkö, joka hyödyntää yhteisiä resursseja ja järjestelmiä riskienhallinnassa
	Jokaisen yksikön oma viitekehys	Hyödynnetään yhtenevää kehystä sovittuihin sääntöihin ja vastuisiin: Petokset ja kyberturvallisuus yhdistyvät ennaltaehkäisyn vaiheessa, esim. asiakkaan tunnistamisessa	Yhtenäinen kuva asiakkaista ja yhtenäiset analytiikkatyökalut
	+ Vähiten ”hajottava”: säilyttää nykytilanteen	Yhtenäiset prosessit riskien tunnistamiseen ja arviointiin	+ Taustalla olevat riskit yhdistyvät
	+ Sääntelyviranomaiset tutuimpia tämän mallin kanssa	Samankaltaiset prosessit, esim. estämisen toiminnoissa	+ Paremmat mahdollisuudet houkutella ja sitouttaa osaajia
	- Huonompi läpinäkyvyys talousrikollisuuden kokonaisriskeihin	+ Yhtenäinen lähestymistapa, pienempi riski mallin päällekkäisyyksille ja aukoille	+ Yhtenäinen tekemisen viitekehys
	- Ei skaalautumisen hyötyä	+ Johdonmukainen organisaatiorakenne nykytilan säilyttämiseksi	+ Skaalautumisen hyödyt keskeisten roolien parissa
	- Pienemmillä yksiköillä voi olla vaikeuksia houkutella osaajia	+ Vähäisempi muutos nykytilasta	- Vaatii suurta organisaatiomuutosta
		- Säilyttää erillisen raportoinnin, joka ei lisää läpinäkyvyyttä	- Vaikka riskit lähentyvät toisiaan, ne ovat silti erillisiä
		- Ei skaalautumisen hyötyä	- Sääntelyviranomaisille vieras malli
		- Pienemmät yksiköt houkuttelevat vähemmän osaajia	

Taulukko 5: Integraatiomallit organisaatioihin (mukaillen Hasham, Joshi & Mikkelsen 2019, 5)

Yhteistyötä korostava malli on useimpien pankkien nykytila. Tässä mallissa jokainen yksikkö, eli talousrikokset, petokset ja kyberturvallisuus, säilyttävät itsenäiset roolinsa, vastuunsa sekä raportoinnin mallin. Jokaista yksikköä kohden luodaan siis oma itsenäinen toiminnan viitekehys ja hyödynnetään yhteistyötä tietojen ja analytiikan osalta transaktioiden seurannassa, petoksissa ja esimerkiksi tietoturvaloukkauksissa. Lisäksi riskien luokittelu ja jaottelu eri kategorioihin tehdään yhteistyössä. Tämä malli on usein tuttu myös sääntelyviranomaisille, mutta se tarjoaa pankeille vain vähän sellaista läpinäkyvyyttä, jota tarvitaan talousrikosten riskien kokonaisvaltaisen kuvan hahmottamiseen. Yhteistyöhön perustuva malli saattaa myös usein epäonnistua saavuttamaan skaalautumisen hyödyt ja johtaa kattavuusaukkoihin sekä päällekkäisyyksiin eri ryhmien välillä. Mallin perustuminen pienempiin ja erillisiin

yksiköihin johtaa myös usein siihen, että pankit eivät kykene houkuttelemaan tarpeeksi korkeatasoista osaamista osaksi henkilöstöään. Osittain integroidussa mallissa yhdistetään kyberturvallisuuden ja petoksien ulottuvuudet. Monet finanssialan toimijat ovat omaksumassa parhaillaan tätä mallia, jossa kyberturvallisuus ja petokset ovat osittain integroituja. Osittain integroidussa mallissa jokainen yksikkö, eli talousrikollisuus, petokset ja kyberturvallisuus, säilyttävät itsenäiset asemansa, mutta toimivat kuitenkin yhtenäisen viitekehyksen alla hyödyntäen yhtenäistä riskien luokittelua ja jaottelua yhteisesti sovittujen sääntöjen pohjalta. Mallissa otetaan käyttöön yhtenäinen lähestymistapa ennaltaehkäisyn toimintamalleihin, riskien tunnistamiseen ja arviointiin ja estämisen prosesseihin liittyen. Etuina tässä mallissa on uhkien seurannan ja havaitsemisen johdonmukaisuus sekä alhaisempi riski mahdollisille malleille ominaisille aukoille tai päällekkäisyyksille. Mallin lähestymistapa on kuitenkin yleensä yhteensopiva nykyisen organisaatiorakenteen kanssa, eikä häiritse tai hajota nykyisiä toimintoja merkittävästi. Toisaalta mallissa läpinäkyvyyden määrä ei myöskään lisäänny, koska raportointi on edelleen erillistä toimintaa. Skaalautumisen etua ei myöskään synny, ja malli ei välttämättä houkuttele korkeasti koulutettua ja osaavaa henkilöstöä pienempien operatiivisten yksiköiden ollessa edelleen olemassa. Kokonaan integroidussa mallissa talousrikokset, petokset ja kyberturvallisuuden toiminnot yhdistetään yhteen toimintakehykseen, jossa hyödynnetään yhteisiä resursseja ja järjestelmiä riskien hallintaan koko organisaatiossa. Mallissa käytetään yhtä yhtenäistä kuvaa asiakkaista jakaen analytiikkaa. Riskien liukuessa lähemmäksi toisiaan niiden ollessa keskinäisessä vuorovaikutuksessa koko organisaation laajuinen läpinäkyvyys uhkien suhteen kasvaa. Tämä paljastaa tehokkaammin taustalla olevat konkreettisimmat riskit. Kokonaan integroitu malli hyödyntää myös skaalautumisen etua keskeisten roolien parissa ja parantaa siten pankin kykyä houkutella ja sitouttaa osaavaa henkilöstöä. Tämän mallin haittapuolina ovat kuitenkin merkittävät organisaatiomuutokset, jotka osaltaan tekevät pankkien toiminnoista vieraampia sääntelyviranomaisille. Riskien keskinäisestä vuorovaikutuksesta huolimatta ne pysyvät kuitenkin myös erillisinä.[125]

Analytiikan hyödyntämisen ja organisaation kehittämisen lisäksi riskienhallinnassa ja muuttuvan toimintaympäristön haasteisiin vastatessa oleellista on myös muu teknologia. Tekoäly ja siihen kuuluvat koneoppimistekniikat muokkaavat perustavanlaatuisesti rahoitusalan lähestymistapoja riskienhallintaan. Esimerkiksi lainapäätökset, varoitusmerkit riskeistä, erilaistenhuijauksien havaitseminen ja malliriskien tunnistaminen ovat osa rahoitusalan riskien tunnistamista ja hallitsemista. Vastaaviin seikkoihin ja erilaisiin rahoitusalan turvallisuusriskeihin tekoäly ja sen luomat mahdollisuudet tarjoavat monenlaisia ratkaisuja.[126] Rahoitusalan toimijoiden kohtaamien operatiivisten riskien määrä ja monimuotoisuus ovat lisääntyneet. Operatiivisen riskienhallinnan tarkoituksena on tunnistaa mahdollisen taloudellisen menetyksen

[125] Hasham, Joshi & Mikkelsen 2019, 6–7.
[126] Aziz & Dowling 2019, 34.

riski, joka johtuu operatiivisista häiriöistä.[127] Ulkoisista tapahtumista aiheutuviin operatiivisiin riskeihin kuuluvat mm. petokset ja järjestelmien haavoittuvuudet. Tekoäly avustaa rahoitusalan toimijoita eri vaiheissa riskienhallintaprosessia tunnistamisesta, mittaamisesta ja arvioimisesta aina vaikutusten seurantaan asti.[128]

Tekoälyteknologia pyrki alun perin ehkäisemään ulkoisia tappioita, jotka johtuivat esimerkiksi luottokorttipetoksista. Nyt teknologia on kuitenkin laajentunut myös toistuvien prosessien suorittamiseen, erilaisten asiakirjakokoelmien analysointiin sekä rahanpesun havaitsemiseen. Taloudellisten petoksien havaitsemisessa hyödynnetään myös koneoppimista ja tekoälyä osana riskienhallintaa. Erilaisten teknologioiden avulla arvioidaan parhaita strategioita suojata järjestelmiä, tietoja ja asiakkaita. Samanaikaisesti tekoäly nopeuttaa erilaisten rutiinitöiden tahtia minimoiden virheet, seuloen pois asiaankuulumattoman sisällön ja määrittelemällä yksilöiden välisiä yhteyksiä arvioiden riskialttiita asiakkaita tai verkostoja.[129] Yhtenä esimerkkinä tekoälyn hyödyntämisestä rahoitusalan turvallisuuden varmistamisessa on kuuden suuren pohjoismaisen pankin vuonna 2019 perustama yhteinen rahanpesun vastainen infrastruktuuri, Nordic KYC utility. Yhteistyössä mukana ovat Danske Bank A/S, DNB Bank ASA, Nordea Bank Abp, Skandinaviska Enskilda Banken AB (publ), Svenska Handelsbanken AB (publ) ja Swedbank AB (publ). Pankkien tavoitteena oli kehittää pohjoismainen alusta standardisoiduille prosesseille liittyen KYC (Know Your Customer) tietojen käsittelyyn. Yhteistyön tarkoituksena on myös ehkäistä rikollisuutta Pohjoismaissa sekä parantaa yritysasiakkaiden asiakaskokemusta yksinkertaistamalla KYC-prosesseja. Tekoälyyn perustuva infrastruktuuri auttaa pankkeja noudattamaan KYC-sääntelyä ja välttämään sääntelyn noudattamatta jättämisestä johtuvia sakkomaksuja.[130]

Aiemmin mainittujen talousrikosten, petoksien ja kyberuhkien integraation avulla voidaan hyödyntää täysimääräisemmin myös pankin tietoja ja automaatiota sekä mahdollistaa tekoälylle ja koneoppimiselle kattavammat tiedot tehokkaampaan ennakoivaan analytiikkaan. Teknologia tuottaa tietoa esimerkiksi tilien kaappausten todennäköisyydestä ja rikollista alkuperää olevien rahasiirtojen yhteyksistä, ja algoritmien tuottamien väärien positiivisten havaintojen määrää voidaan laskea yhdistämällä nämä tiedot teknologian sääntöpohjaisiin ratkaisuihin. Tällaiset ratkaisut alentavat myös pankkien kustannuksia ja jättävät resursseja muiden tapahtumien selvittelyyn ja ratkomiseen. Esimerkiksi eräs maailmanlaajuisesti toimiva pankki on yhdistänyt kaikki talousrikoksiin liittyvät toimintonsa yhdeksi kokonaisuudeksi. Toimimalla näin tämä kyseinen pankki on saanut ensinnäkin kokonaisvaltaisemman kuvan asiakasriskistään ja kaiken lisäksi vähentänyt omia käyttökustannuksiaan noin 100 miljoonalla

[127] Aziz & Dowling 2019, 43 mukaan Moosa 2007.
[128] Aziz & Dowling 2019, 43 mukaan Sanford & Moosa 2015.
[129] Aziz & Dowling 2019, 43–44.
[130] Nordea 2019. Ks. myös Aziz & Dowling 2019, 44.

dollarilla. Finanssialan kohtaamien riskien monimutkaistuessa pankkien toimintojen huomataankin tulevan kalliimmiksi ja entistä tehottomammiksi. Sen vuoksi onkin aiheellista pohtia uusia lähestymistapoja turvallisuuden varmistamiseksi. Nykyisellään kyberrikollisuuden ja petosten torjuntaan käytettävät keinot ovat keskittyneet pääasiassa pistekohtaisiin kontrolleihin tai organisaation ja hallinnon siiloihin. Nämä keinot eivät kuitenkaan perustu ymmärrykseen siitä, miten rikolliset käyttäytyvät. Jotta rahoitusalan toimijat saisivat realistisemman kuvan tapahtumista, heidän tulisi ajatella itsekin kuin rikolliset: rikollisuus hyödyntää kaikkia heikkoja kohtia järjestelmissä ja prosesseissa. Jos keskitytään parantamaan vaikkapa ainoastaan teknologian toimivuutta, rikollinen toiminta siirtyy muualle, kuten asiakkaisiin. Tämä toisaalta taas pakottaa toimijat yhdistämään eri ulottuvuudet ja teemat yhteneväisemmäksi kokonaisuudeksi. Teknologian monipuolinen hyödyntäminen, eri osaajien sitouttaminen ja saaminen osaksi organisaatiota sekä eri teemojen riskienhallinnan integrointi osaksi omaa liiketoimintaa ja organisaatiorakennetta voi siis olla yksi suuri tulevaisuuden teema rahoitusalalla.[131]

5.2 Identiteettivarkauksista ja rahanpesusta

Henkilöllisyyteen perustuvat rikollisuuden muodot ovat vakava ja kasvava riski monille valtioille ja niiden hallituksille. Identiteettivarkauksien on arvioitu aiheuttavan miljardien dollareiden taloudellista haittaa mm. menetettyjen verotulojen ja liikaa maksettujen sosiaaliturvaetuuksien ja eri alojen toimijoiden kärsimien tappioiden muodossa. Identiteettivarkaudet liittyvät yleensä muuhun petosrikollisuuteen, ja tämäkin rikollisuuden muoto on kehittynyt yhä enemmän organisoidumpaan muotoon. Englanninkielisessä lähdeaineistossa on usein erotettu termit identity theft ja identity fraud. Henkilöllisyyspetoksella (identity fraud) on useimmiten englanninkielisissä aineistoissa viitattu tapahtumaan, jossa jonkun toisen henkilöllisyystietoja tai väärennettyjä henkilötietoja hyödynnetään rikosten tekemisessä tai velvollisuuksien ja vastuiden välttelyssä. Henkilöllisyyden varastamisella (identity theft) viitataan usein tapahtumaan, jossa rikoksentekijä on saanut riittävästi tietoa jonkun toisen henkilöllisyydestä aikomuksenaan käyttää saamiaan tietoja henkilöllisyyspetoksen tekemiseen.[132] Tässä työssä molemmista ilmauksista käytetään kuitenkin suomenkielistä termiä identiteettivarkaus, sillä Suomen rikoslain (39/1889) 38 luvun pykälässä 9 a identiteettivarkaus määritellään toimintana, jossa joku erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa aiheuttaen taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee. Suomenkielinen ilmaus siis kattaa siis molemmat englanninkieliset skenaariot.

---

[131] Hasham, Joshi & Mikkelsen 2019, 9–11.
[132] OECD 2006, 4–5.

OECD:n (Organisation for Economic Co-operation and Development) vuoden 2006 raportissa tutkittiin veronkierron ja rahanpesun haavoittuvuustekijöitä, jotka liittyivät osaltaan identiteettivarkauksiin. Selvityksessä tunnistettiin useita keinoja ja menetelmiä veronkiertoon ja rahanpesuun sekä niihin liittyviin identiteettivarkauksiin. Selvityksessä mukana oli 19 eri maata, osa eurooppalaisia valtioita, osa Etelä-Amerikan valtioita, Aasian sekä Lähi-Idän valtiot.[133] Taulukossa 6 on esitetty selvityksessä esiin tulleita toimintamalleja veronkierron tai rahanpesun järjestämiseksi hyödyntäen väärennettyä tai varastettua henkilöllisyyttä.

Väärän henkilöllisyyden luominen tai jonkun toisen tietojen haltuunotto tarkoituksena tehdä valheellisia valituksia erinäisten palautusten ja hyvitysten saamiseksi (esim. väärennetylle identiteetille valheellisia tietoja hyödyntäen tehty tuloveroilmoitus, jotta saataisiin palautuksia ja hyvityksiä).
Väärennettyjen tai varastettujen henkilöllisyyksien käyttö yritysten perustamiseen ja sitä kautta myös tulovero- tai palautuspetoksiin.
Väärennetyn henkilöllisyyden luominen tai petoksella tai varkaudella haltuun saadun henkilöllisyyden käyttö passin tai muun henkilöllisyysasiakirjan saamiseksi, jotta saataisiin oma henkilötunnus. Tätä henkilötunnusta käytetään taas esim. sosiaaliturvaetuuksien hakemiseen, verotuksellisien asioiden hoitoon, yrityksen perustamiseen ja pankkitilien avaamiseen.
Veroviranomaisten lähettämien kirjeiden ja postin varastaminen ja näissä olevan tiedon hyödyntäminen työllistymistä tai korvausten hakemista varten, esim. lääkärikulut.
Peiteyritysten perustaminen ainoastaan arvonlisäveron hyvityksen tai muiden palautusten saamiseksi. Myös nk. ”karusellihuijaus”, jossa peitefirman johtaja käyttää väärennettyä tai varastettua identiteettiä.
Peiteyritysten perustaminen ja väärennettyjen sekkien hyödyntäminen rahansiirrossa. Sekit on saatu pankeista väärennetyn tai varastetun henkilöllisyyden turvin.
Tavarantoimittajien asiakirjojen vilpillinen käyttö. Tavarantoimittajien kanssa ei todellisuudessa ole tehty kauppaa, ja tarkoituksena on ainoastaan saada alennettua sovellettavaa tuloverokantaa tai luoda keinotekoisia tappioita.
Väärennettyä tai varastettua henkilöllisyyttä käyttävä saattaa olla jonkin pankkitilin omistaja tai näennäisen laillisesti valtuutettu pankkitilin käyttäjä. Tilin käytön tarkoituksena on suurten käteissummien tallettaminen, jotka siirretään edelleen muille tileille useihin eri maihin, ja sieltä rahat siirtyvät edelleen laillisiin yrityksiin.
Maahanmuuttajien henkilöllisyyden käyttö, vaikka kyseiset henkilöt ovat todellisuudessa palanneet kotimaihinsa. Tarkoituksena jatkaa sosiaaliturvaetuuksien hakemista ja vastaanottamista.
Henkilön identiteetin kaappaaminen sellaiselta toimijalta, joka jo käyttää sitä petoksien tekemiseen.

[133] OECD 2006, 4-6.

Edustaja, esimerkiksi asianajaja tai muu toimija esittää vaatimuksia vaikkapa hyvitysten tai etuuksien saamisesta henkilölle, jota todellisuudessa ei ole olemassa.
Pankkitilin avaaminen toiselle henkilölle, joka ei ole pankkitilin avaaja.
Haavoittuvassa asemassa olevien ihmisten hyväksikäyttö, tarkoituksena saada salasanoja ja saada pääsy eri järjestelmiin ja manipuloida toista henkilökohtaisen hyödyn nimissä.
Varkaiden yritykset päästä käsiksi varastoihin, jossa säilytetään henkilöllisyystietoja sisältäviä dokumentteja. Pääsy voi tapahtua hakkeroimisella, korruption tai petoksen avulla. Kohteena ovat usein suuret virastot, kuten pankit tai hallituksen virastot.

Taulukko 6: Toimintamalleja veronkierron tai rahanpesun järjestämiseksi hyödyntäen varastettua tai väärennettyä henkilöllisyyttä[134]

Esimerkiksi Kanadassa väärennettyjä tai varastettuja henkilöllisyystietoja on hyödynnetty yritysten perustamisessa vilpillisten tuloveroilmoituksien tekemiseen ja palautuksien saamista varten. Lisäksi esiin oli noussut tapauksia, jossa veroviranomainen paisutteli asiakkaansa saaman palautuksen summaa ja piti siitä saadun erotuksen itsellään tai käytti vanhoja asiakastietoja vilpillisten ilmoitusten tekemiseen ja palautuksien saamiseen. Ranskassa taas oli tullut ilmi, että identiteettivarkauksia hyödynnetään myös markkinointisektorilla. Tässä petoksessa varastettu tai väärennetty identiteetti liittyi yrityshuijaukseen, jonka avulla oli kiristetty rahaa sellaisilta yrityksiltä, joille vilpillinen mainostoimisto oli myynyt mainostilaa. Joskus myös tällaisen mainostoimiston asiakkaat olivat mukana juonessa hyödyntäen toimintamallia oman veropohjansa alentamiseen. Joskus nämä huijaukset liittyivät myös rahanpesuun. Meksikossa tekijät loivat väärennettyjä henkilöllisyystodistuksia hyödyntäen kolmansilta osapuolilta saatuja tietoja. Henkilöllisyystodistusten avulla perustettiin yrityksiä, avattiin pankkitilejä sekä luotiin erilaisia tekaistuja sopimuksia ja laskuja. Näistä toimista rikolliset eivät ilmoittaneet verohallinnolle mitään tuloja, ja katosivat maksamatta veroja pesettäen laittomista alkuperistä saatua rahaa. Veroviranomaisen havaitessa veronkierron alkoi tutkimus henkilöllisyyden todellisen omistajan kanssa, joka ei tunnistanut tekoja omikseen. Prosessi rikoksentekijän kiinnisaamiseksi tällaisessa tapauksessa on usein pitkä, ja se on horjuttanut kansalaisten luottamusta hallintoon ja aiheuttanut merkittäviä kustannuksia. Yhdysvalloissa varkaat yrittivät päästä käsiksi erilaisiin suuriin henkilöllisyystietoja ylläpitäviin varastoihin hakkeroimalla, petoksien tai korruption avulla. Tällaisia toimijoita, jotka säilyttävät henkilötietoa olivat esimerkiksi pankit, hallituksen virastot, luottotietoyhtiöt ja internetissä toimivat yhtiöt, jotka vaativat asiakkaidensa henkilötietoja palveluiden avaamiseksi. Suurilla yrityksillä ja toimijoilla on monenlaisia asiakirjoja, kuten työhakemuksia, palkka-asiakirjoja sekä muuta

[134] Tiedot taulukossa OECD 2006, 6.

henkilöstöön liittyvää tietoa sisältäviä asiakirjoja, joita voitiin hyödyntää henkilöllisyystietojen varastamisessa.[135]

Suomalaisesta oikeuskäytännöstä ei löytynyt tapauksia, jossa tekijä olisi tuomittu sekä identiteettivarkaudesta että rahanpesusta. Muualta maailmalta esimerkkejä löytyy runsaammin. Esimerkiksi Yhdysvalloissa vuonna 1999 Patrick Penker niminen mies osti kassasekin American State Bankin haarakonttorista, joka oli osoitettu nimelle Howie Dewey Cheatham. Käytetty nimi oli muunnelma suositusta komediasarjasta The Three Stooges, jossa erään lakifirman nimi oli Dewey, Cheatham & Howe. Seuraavana vuonna Penkerin yrittäessä uusia kassasekkiään, pankin työntekijä huomasi tunnisti väärän nimen ja ilmoitti tapauksesta FBI:lle. Selvisi, että Penker oli vuosien saatossa käyttänyt useita eri nimiä ja sosiaaliturvatunnuksia saadakseen luottokortteja ja lainoja keräten varallisuutta näiden avulla yli miljoona dollaria. Penker tunnusti syyllisyytensä rahanpesuun ja identiteettivarkauteen.[136]

Erilaiset petokset ja järjestäytynyt rikollisuus, kuten rahanpesu, terrorismi ja laiton maahanmuutto ovat yleensä identiteettivarkauksien vakavimpia seurauksia. Identiteettivarkaudet ja vastaavat petokset tulevat kalliiksi yhteiskunnille. Asuntolainapetokset ovat myös olleet yksi huolestuttava petoksen muoto, joka on seurausta identiteettivarkaudesta. Asuntolainapetoksessa hyödynnetään väärennettyä tai varastettua henkilöllisyyttä asuntolainan saamiseksi. Yhdysvalloissa asuntolainapetokset kasvoivat 500 prosentilla vuosien 2001–2004 välillä. Kanada taasen menetti tarkasteluvuonna 2012 vuosittain suunnilleen 1,5 miljoonaa dollaria asuntolainapetoksiin. Vuonna 2006 Brittiläisessä Kolumbiassa sijaitsevassa Surreyssä eräs nainen esiintyi kiinteistön omistajana hakien 170 000 dollarin asuntolainaa. Lainaneuvottelija järjesti lainan, mutta toinen neuvottelija huomasi huijauksen ja ilmoitti siitä poliisille. Tekijät hyödyntävät väärennettyjä tai varastettuja henkilöllisyystodistuksia, tuloilmoituksia sekä työhistoria tietoja tarkoituksenaan saada asuntolaina uhrin luottotietojen avulla tai omistaa kiinteistöjä ja myydäkseen niitä sitten eteenpäin. Ottawan poliisin mukaan asuntolainapetoksiin liittyy usein huumausainerikollisuutta. Huumekauppiaat saavat kiinteistöjä omistukseensa asuntolainapetoksien avulla ja käyttävät kiinteistöjä huumausainerikollisuuden järjestämiseen ja toteuttamiseen, esimerkiksi kasvattamalla marihuanaa kiinteistössä.[137]

6 Yhteenveto ja johtopäätökset

[135] OECD 2006, 7.
[136] Wall Street Journal 2001.
[137] Hedayati 2012, 3–5.

Tämän opinnäytetyön tavoitteena oli tutkia identiteettivarkauksia ja rahanpesua ilmiöinä pääasiassa lainopillisesta näkökulmasta sekä näiden ilmiöiden vaikutusta finanssialan turvallisuuteen. Lisäksi työn tavoitteena oli kartoittaa strategioita finanssialan turvallisuuden parantamiseksi ottaen huomioon teknologian luomat mahdollisuudet uudenlaisten kyber-, talous- ja petosrikosten ollessa kasvava ongelma finanssialan turvallisuudelle. Työssä analysoitiin identiteettivarkauksien asemaa osana suomalaista lainsäädäntöä, identiteettivarkauksien esiintymistä käytännössä, ilmiön yleisyyttä sekä sen asemaa osana muuta kyberrikollisuutta pääasiassa kotimaisessa kontekstissa. Työssä syvennyttiin myös tutkimaan rahanpesun asemaa osana suomalaista lainsäädäntöä, rahanpesun esiintymistä käytännössä sekä sen yleisyyttä ja asemaa osana talousrikollisuutta keskittyen kotimaiseen kontekstiin. Lisäksi työssä tuotiin ilmi finanssialan kohtaamia turvallisuushaasteita, jotka pohjautuvat nykyteknologian mahdollistamista keinoista toteuttaa kyber-, talous- ja petosrikollisuutta uusin tavoin. Työssä käytiin läpi myös strategioita finanssialan turvallisuuden parantamiseksi sekä viimeisenä tuotiin esiin identiteettivarkauksien ja rahanpesun yhteyttä ja esimerkkitapauksia maailmalta, jotta kaikkien käsiteltyjen aiheiden kokonaisuus olisi eheä ja asioiden merkitys toisiinsa nähtäisiin myös suuremmassa mittakaavassa.

Työn rajoituksina olivat tiettyjen aiheiden kuuluminen ainoastaan kotimaiseen kontekstiin ja muiden aiheiden liittyminen enemmän kansainväliseen kontekstiin. Esimerkiksi tietoa talous- ja petosrikollisuuden siirtymisestä verkossa toteutettavaan muotoon löytyi vain kansainvälisestä kontekstista. Alan toimijoiden sääntelyssä ja regulaatiossa ylipäätään voi olla pieniä eroavaisuuksia eri puolilla maailmaa, ja strategioiden tehokkaaseen implementointiin voivat vaikuttaa myös muut alan organisaatioihin ja yrityksiin lukeutuvat seikat, kuten maantieteellinen sijainti, toiminnan muoto sekä laajuus ja paikallinen sääntely. Kaikkia tutkimuksen havaintoja ei siis välttämättä voida suoraan yhdistää esimerkiksi Suomen kontekstiin. Samaten tietoa identiteettivarkauksien, veronkierron ja rahanpesun yhteydestä löytyi vain kansainvälisestä kontekstista, vaikka osa saaduista tiedoista sijoittuikin Euroopan alueelle. Työssä hyödynnettyä lähdeaineistoa on pyritty tarkastelemaan mahdollisimman puolueettomasti ja kaikki käytetty lähdeaineisto on merkitty alaviittein. Opinnäytetyön tulokset on raportoitu totuudenmukaisesti.

Opinnäytetyön tuloksina tuli ilmi petosrikollisuuden määrän voimakas kasvu sekä sen yhteys kansainväliseen rikollisuuteen, kuten järjestäytyneiden rikollisryhmien toimintaan, suurempiin petoskokonaisuuksiin tai jopa rahanpesuun. Myös identiteettivarkauksilla oli usein yhteys muuhun petosrikollisuuteen, yleisimmin maksuvälinepetoksiin tai muihin petosvyyhteihin. Suurin osa petoksista tapahtuu nykyään tietoverkkoavusteisesti, ja työssä esitettiin myös riskitekijöitä verkossa tapahtuvien rikosten uhriksi joutumiselle. Riskitekijöinä olivat mm. verkon ja muun teknologian aktiivinen käyttö, aiempi offline uhriksi joutuminen sekä hyvä taloudellinen tilanne. Lisäksi vanhempaan ikäluokkaan kuuluvat miehet olivat muita enemmän alttiita huijauksille sekä haittaohjelmien toiminnalle. Tuloksissa ilmeni myös, että rahanpesulla oli

voimakas yhteys korruptioon Euroopan Unionin alueella, ja toiminta on siirtynyt entistä organisoidumpaan, järjestäytyneeseen muotoon. Rahanpesun yleisyyttä ja tarkkaa määrää on hankala arvioida, sillä se liittyy usein erilaiseen järjestäytyneeseen rikollisuuteen. Euroopan Unionin alueella toimivista rikollisjärjestöistä n. 70 % hyödyntää rahanpesua toimintansa jatkamisessa ja varojen alkuperän häivyttämisessä, ja samaisista järjestöistä 60 % hyödyntää korruptiota rikollisen toimintansa mahdollistajana. Toisaalta rahanpesu voi ilmetä myös hyvin pienimuotoisena toimintana, kuten varastetun tavaran kauppaamisena eteenpäin. Suomessa vuodesta 2015 eteenpäin rahanpesun yleisimpiin esirikoksiin lukeutuivat petosrikokset, kun taas aiemmin tyypillisimpiä esirikoksia olivat huumausainerikokset ja talousrikokset.

Työssä huomattiin myös, että teknologian kehityksellä on vaikutusta rikollisuuden kehittyneisyyteen. Tätä tukee myös petosrikollisuuden muuttuminen lähes poikkeuksetta tietoverkkoavusteiseksi rikollisuudeksi sekä rahanpesun toteuttaminen tietoverkkoja hyödyntäen. Lainsäädännön jatkuvalla päivittämisellä pyritään pysymään teknologian sekä rikollisen toiminnan kehityksen kannoilla. Lisäksi Rahanpesun selvittelykeskuksen vastaanottamista ilmoituksista vähintään neljäsosa liittyi petosrikollisuuteen, jolloin petosrikollisuuden liittyminen suurempiin vyyhteihin, toiminnan kansainvälistyminen sekä yhteys rahanpesuun on huomattu myös Suomessa. Finanssialan turvallisuutta tutkittaessa tuli ilmi, että talous- ja petosrikollisuudella on yhteyttä kyberrikollisuuteen alan kohtaamien turvallisuusuhkien näkökulmasta, ja osa suurimmista alan toimijoista on jo kiinnittänyt huomiota tähän ilmiöön osana strategista toimintaansa ja asiakastyytyväisyyttä. Työssä huomattiin siis, että talous-, petos- ja kyberrikollisuuden ulottuvuuksien yhteen tuominen ja ilmiöiden liittyminen toisiinsa on tärkeä tunnistaa, jotta turvallisuusuhkiin puuttuminen olisi tehokkaampaa. Usein näin suuressa mittakaavassa tapahtuva rikollisen ympäristön muuttuminen kehittyneempään suuntaan vaatinee siis myös organisaatiotason muutoksia, osaavaa ja sitoutunutta henkilöstöä, huomion kiinnittämistä hallintojen ja organisaatioiden siiloutumiseen sekä teknologian, analytiikan ja tekoälyn hyödyntämistä niin mobiili- kuin verkkopankkiympäristöjen turvallisuusseikkojen parantamiseen kuin prosessien virtaviivaistamiseenkin. Lisäksi työssä tuotiin esiin identiteettivarkauksien hyödyntämistä osana veronkiertoa ja rahanpesurikollisuutta, ja toiminta oli usein hyvin monimuotoista ja siinäkin oli huomattavissa petosrikollisuuden piirteitä.

Opinnäytetyön tuloksista voi olla hyötyä finanssialan toimijoille, asiakkaille kuin muillekin yhteiskunnan jäsenille. Aihe on ajankohtainen, sillä petos- ja verkkorikollisuuden voimakas kasvu koskettaa myös tavallisia kansalaisia, ja työssäkin esiin nousi, että keskiössä näiden rikosten ehkäisyssä ja estämisessä on olennaisesti kansalaisten oma tarkkaavaisuus ja aktiivisuus tunnistaa näitä rikoksia. Vaikka petosrikollisuudessa omaisuuden takaisinsaannin mahdollisuudet ovat usein pienet, niistä kannustetaan tekemään rikosilmoitus, sillä petokset voivat liittyä suurempiin petosvyyhteihin tai tekijällä voi olla myös monia muita uhreja. Ilmoitusten teon avulla viranomaiset saavat myös kattavamman kuvan ilmiöstä ja tekijöiden kiinnijäämisen mahdollisuudet kasvavat. Näiden seikkojen vuoksi tiedon lisääminen aiheista on tärkeää,

sillä petosrikollisuus on tullut jäädäkseen. Suomessakin poliisihallintoon perustetaan oma yksikkö, joka tutkii jatkossa tietoverkkoavusteisia petoksia. Ilmiön laajuuden tunnistaminen on siis olennaista.

Yhteenvetona käsitellyistä aiheista voidaan siis todeta, että petosrikollisuuden kasvu on todellinen turvallisuusuhka sekä kansalaisille, että finanssialan toimijoillekin. Talous- ja petosrikollisuuden siirtyminen verkossa tapahtuvaan muotoon on tärkeä ottaa huomioon kansalaisten valistamisessa, tiedon lisäämisessä mutta myös finanssialan toimijoiden keskuudessa heidän pohtiessaan strategioita turvallisuuden ja asiakastyytyväisyyden kehittämiseksi. Käsiteltyjen aiheiden yhteydet ovat myös tärkeä tunnistaa, sillä rikollisuus kehittyy yhtä nopeasti kuin uusimmat teknologiatkin, jolloin turvallisuudesta huolehtiminen vaatii monipuolisia ja hallinnollisia toimenpiteitä sekä tarpeeksi nopeasti ja tehokkaasti päivittyvää lainsäädäntöä. Uudentyyppisen rikollisuuden tunnistaminen ja ehkäisy finanssialalla vaatinee siis sekä alan toimijoiden viranomaisten kuin teknologiayritystenkin tiivistä yhteistyötä. Lainsäädännön ja siihen liittyvien prosessien tulisi myös olla tarpeeksi joustavia, jotta sääntely pysyisi teknologian nopean kehityksen kannoilla tarpeeksi tehokkaasti. Finanssialan toimijoiden tulisi myös pohtia teknologisia ratkaisuja ja strategioita erilaisten uhkien ja skenaarioiden varalle. Jatkotutkimusaiheita pohjautuen tässä työssä käsiteltyihin aiheisiin voisivat olla petos- ja rahanpesurikollisuuden yhteyden tutkiminen finanssialan kontekstissa sekä lainsäädännön tehokkuuden ja nopeuden arviointi liittyen tämäntyyppisiin rikoksiin. Lisäksi myös muunlaisia strategioita, niiden implementointia ja tehokkuutta finanssialan turvallisuuden parantamiseksi voisi olla syytä tarkastella yksityiskohtaisemmin.

Lähteet

Kirjallisuus ja artikkelit

Aziz, S. & Dowling, M. 2019. Machine Learning and AI for Risk Management. Teoksessa Lynn, T., Mooney, J., Rosati, P. & Cummins, M. Disrupting Finance. Palgrave Studies in Digital Business & Enabling Technologies. Viitattu 14.5.2024. https://doi.org/10.1007/978-3-030-02330-0_3

Boucht, J. & Frände, D. 2019. Suomen rikosoikeus: Rikosoikeuden yleisten oppien perusteet. Suomentanut Markus Wahlberg. 2. painos. Tampere: Poliisiammattikorkeakoulu. Viitattu 4.5.2024. https://urn.fi/URN:ISBN:978-951-815-356-9

Ervasti, K. 2011. Oikeustiede – Jurisprudentia XLIV. Oikeussosiologia ja oikeuspoliittinen tutkimus osana oikeustiedettä. Suomalaisen lakimiesyhdistyksen vuosikirja 44. Helsinki: Suomalainen lakimiesyhdistys, 61–132.

Ervasti, K. 2022. Yhteiskunnallinen oikeustutkimus. Gaudeamus. E-kirja.

Hedayati, A. 2012. An analysis of identity theft: Motives, related frauds, techniques and prevention. Journal of Law and Conflict Resolution 4(1), 1-12. https://academicjournals.org/journal/JLCR/article-abstract/8599A6F7684

Hirvonen, A. 2011. Mitkä metodit? : opas oikeustieteen metodologiaan. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja. Yleisen oikeustieteen julkaisuja; 17. Helsinki: Helsingin yliopisto. Viitattu 10.5.2024. http://hdl.handle.net/10138/225264

Husa, J., Mutanen, A. & Pohjolainen, T. 2001. Kirjoitetaan juridiikkaa. Helsinki: Talentum Media.

Hyttinen, T. 2017. Rahanpesun esirikoksen toteennäyttämiskynnys. Defensor Legis 6/2017. Helsinki: Suomen asianajajaliitto, 833–851. Viitattu 11.4.-15.4.2023. https://urn.fi/URN:NBN:fi-fe2021042717747

Korkka-Knuts, H., Frände, D. & Helenius, D. 2020. Yleinen rikosoikeus. Edita Publishing. E-kirja. Viitattu 4.5.2024.

Luoto, L. 2022. Lainkonkurrenssin ratkaisukriteerit KKO:n tuoreen oikeuskäytännön ja oikeustieteen valossa. Defensor Legis 2/2022. Helsinki: Suomen asianajajaliitto, 403–418. https://urn.fi/URN:NBN:fi-fe2022081153646

Matikkala, J., Frände, D., Kekkonen, J., Lahti, R., Lappi-Seppälä, T., Majanen, M., Marttunen, M., Melander, S., Nordenstreng, K. & Nuotio, K. 2013. Rikosoikeuden muutos 190-luvulta 2010-luvulle. Pekka Koskisen (1943–2011) muistojulkaisu. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut. Helsinki: Helsingin yliopisto. Viitattu 4.5.2024. http://hdl.handle.net/10138/225282

Näsi, M., Danielsson, P. & Kaakinen, I. 2022. Cybercrime Victimisation and Polyvictimisation in Finland-Prevalence and Risk Factors. European Journal on Criminal Policy and Research, 29(2), 283–301. https://doi.org/10.1007/s10610-021-09497-0

Sahavirta, R. 2008. Rahanpesu rangaistavana tekona. Suomalaisen lakimiesyhdistyksen julkaisuja. A-sarja N:o 286. Helsinki: Suomalainen lakimiesyhdistys. Viitattu 16.4.-9.5.2024. https://edition.fi/lakimiesyhdistys/catalog/view/525/440/1037-1

Siltala, R. 2003. Oikeustieteen tieteenteoria. Suomalaisen lakimiesyhdistyksen julkaisuja. A-sarja N:o 234. Helsinki: Suomalainen lakimiesyhdistys. Viitattu 10.5.2024. https://edition.fi/lakimiesyhdistys/catalog/book/537

Tuori, K. 2013. Oikeusjärjestys ja oikeudelliset käytännöt. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja. Helsinki: Helsingin yliopisto. Viitattu 10.5.2024. https://doi.org/10.31885/9789515182630

Virallislähteet

HE 94/1993 vp. Hallituksen esitys Eduskunnalle rikoslainsäädännön kokonaisuudistuksen toisen vaiheen käsittäviksi rikoslain ja eräiden muiden lakien muutoksiksi.

HE 232/2014 vp. Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräiksi siihen liittyviksi laeiksi.

HE 9/2018 vp. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi.

HE 53/2002 vp. Hallituksen esitys Eduskunnalle eräiden rikoslain talousrikossäännösten ja eräiden niihin liittyvien lakien muuttamiseksi.

HE 285/2010 vp. Hallituksen esitys Eduskunnalle laeiksi rikoslain 32 luvun 6 ja 14 §:n sekä kansainvälisestä oikeusavusta rikosasioissa annetun lain 15 §:n muuttamisesta.

LaVM 22/1994 vp. Lakivaliokunnan mietintö n:o 22 hallituksen esityksestä rikoslainsäädännön kokonaisuudistuksen toisen vaiheen käsittäviksi rikoslain ja eräiden muiden lakien muutoksiksi.

LaVM 29/2014 vp. Lakivaliokunnan mietintö 29/2014 vp. Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräiksi siihen liittyviksi laeiksi.

Muut lähteet

Andström, K. 2003. Perusasioita oikeustieteestä. Viitattu 11.4.2024. https://www.avoin.helsinki.fi/oppimateriaalit/oikeustiede/materiaali/

Arman, M. 2023. Money Laundering: A Three Step Secret Game. Partners Universal International Innovation Journal (PUIIJ), 01(01), 34–45. https://doi.org/10.5281/zenodo.7644399

Čihák, M. & Tieman, A. 2008. Quality of Financial Sector Regulation and Supervision Around the World. IMF Working Paper WP/08/190. International Monetary Fund. Viitattu 13.5.2024. https://doi.org/10.4337/9781849805766.00022

Euroopan unionin neuvosto 2024a. Rahanpesun torjunta: neuvosto ja parlamentti sopuun tiukemmista säännöistä. Viitattu 9.5.-10.5.2024. https://www.consilium.europa.eu/fi/press/press-releases/2024/01/18/anti-money-laundering-council-and-parliament-strike-deal-on-stricter-rules/pdf/

Euroopan unionin neuvosto 2024b. Viitattu 10.5.2024. https://www.consilium.europa.eu/fi/press/press-releases/2024/02/22/frankfurt-to-host-the-eus-new-anti-money-laundering-authority-amla/

Euroopan unionin virallinen lehti (EUVL) L 150 2023, 36. Viitattu 10.5.2024. https://eur-lex.europa.eu/eli/reg/2023/1113/oj

Euroopan tilintarkastustuomioistuin 2021. EU:n toimet rahanpesun torjumiseksi pankkisektorilla ovat hajanaisia ja täytäntöönpano on riittämätöntä. Erityiskertomus 13/2021. Viitattu 9.5.2024. https://op.europa.eu/webpub/eca/special-reports/fight-money-laundering-13-2021/fi/

Europol 2024a. Euroopan unionin talousrikollisuutta koskeva uhkakuva-arvio – Tiivistelmä. Viitattu 11.4.2024-15.5.2024. https://www.europol.europa.eu/publications-events/publications/other-side-of-coin-analysis-of-financial-and-economic-crime

Europol 2024b. Viitattu 9.5.2024. https://www.europol.europa.eu/crime-areas/economic-crime/money-laundering

FATF 2024. Annual Report 2022-2023. Viitattu 15.4.-19.4.2024. https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/FATF-Annual-Report-2022-2023.pdf.coredownload.pdf

Finanssivalvonta 2024a. Viitattu 11.4.2024. https://www.finanssivalvonta.fi/rahanpesun-estaminen/

Finanssivalvonta 2024b. Viitattu 14.5.2024. https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/lehdistotiedotteet/2024/maksamiseen-liittyvat-petokset-ja-huijaukset-kasvava-ilmio--finanssivalvonnan-selvityksen-mukaan-pankkiasioinnin-turvallisuutta-mahdollisuus-parantaa/

Finanssivalvonta 2022. Rahanpesun ja terrorismin rahoittamisen estämisen ja talouspakotteiden noudattamisen valvontastrategia. Viitattu 19.4.2024. https://www.finanssivalvonta.fi/globalassets/fi/rahanpesun-estaminen/rahanpesun_valvontastrategia_16122022_final.pdf

Hakkarainen, L. 2020. Turvaverkko 2.0. Haaste lehti 1–2/2020. Oikeusministeriö ja Rikoksentorjuntaneuvosto, 18–20. Viitattu 24.5.2024. https://rikoksentorjunta.fi/documents/5235988/56402368/2020-1-2_Haaste.pdf/0ecd2c1c-bf1b-137d-29c3-032b732b6b84/2020-1-2_Haaste.pdf?t=1617029567310

Hampton, M. & Levi, M. 1999. Fast spinning into oblivion? Recent developments in money-laundering policies and offshore finance centres. Third World Quarterly, 20(3), 645–656. https://doi.org/10.1080/01436599913730

Hasham, S., Joshi, S. & Mikkelsen, D. 2019. Financial crime and fraud in the age of cybersecurity. McKinsey & Company. Viitattu 13.5.-15.5.2024. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity

Heikkilä, I. 2022. Rahanpesurikokset oikeuskäytännössä – Törkeät rahanpesutuomiot Helsingin hovioikeudessa 2019–6/2022. Keskusrikospoliisi. Viitattu 15.4.-16.4.2024. https://poliisi.fi/documents/25235045/67733116/Rahanpesurikokset-oikeuskaytannossa-2022.pdf/9be02a70-70d0-2e28-edb2-f64fdb25ecd5/Rahanpesurikokset-oikeuskaytannossa-2022.pdf?t=1669617362516

Heikkilä, I. 2023. Rahanpesun ja terrorismin rahoittamisen indikaattorit. Keskusrikospoliisi. Viitattu 5.5.2024. https://poliisi.fi/documents/25235045/67733116/Rahanpesun-ja-terrorismin-rahoittamisen-indikaattorit-2022.pdf/b77ec2e8-df6b-bfbd-3ecb-d1729814a88c/Rahanpesun-ja-terrorismin-rahoittamisen-indikaattorit-2022.pdf?t=1678089581643

IMF 2022. IMF on maailmanlaajuista rahapolitiikkaa ja taloudellista vakautta edistävä kansainvälinen järjestö. Viitattu 13.5.2024. https://www.imf.org/en/Countries

Kallio, R. 2021. Identiteettivarkaus – uhrin myötävaikutus ja tekijän rikosoikeudellinen vastuu. Pro gradu -tutkielma. Turun yliopiston oikeustieteellinen tiedekunta. Turku. Viitattu 9.2.2024. https://urn.fi/URN:NBN:fi-fe2021042311633

Kolttola, I. & Näsi, M. 2022. Suomalaiset väkivallan ja omaisuusrikosten kohteena 2021 : Kansallisen rikosuhritutkimuksen tuloksia. Katsauksia 51/2022. Helsinki: Helsingin yliopisto. Viitattu 11.4.2024. http://hdl.handle.net/10138/348246

Koponen, M. 2023. Maailmantilanne vaatii finanssialalta valppautta. Finanssivalvonta. Viitattu 14.5.2024. https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/blogit/2023/maailmantilanne-vaatii-finanssialalta-valppautta/

KPMG 2023. Rising Financial Crime Risks in Digital Payments. Viitattu 29.4.2024-15.5.2024. https://kpmg.com/us/en/articles/2023/rising-financial-crime-risks-digital-payments.html

Kyberturvallisuuskeskus 2023. Identiteettivarkaudet ja tietojenkalastelu verkossa. Viitattu 20.2.2024-15.5.2024. https://www.kyberturvallisuuskeskus.fi/fi/identiteettivarkaudet-ja-tietojenkalastelu-verkossa

Nordea 2019. The collaboration of six Nordic banks results in a joint KYC company. Viitattu 14.5.2024. https://www.nordea.com/en/doc/1073764.pdf

Näsi, M. 2022. Rikollisuustilanne 2021 : rikollisuuskehitys tilastojen ja tutkimusten valossa. Teoksessa Kolttola, I., Suonpää, K., Raeste, A., Malin, T., Vauhkonen, T., Latvala, A., Anning, L., Sutela, M., Kaakinen, M. & Kivivuori, J. Katsauksia 52/2022. Helsinki: Helsingin yliopisto. Viitattu 5.3.-15.5.2024. http://hdl.handle.net/10138/352005

Näsi, M. & Tanskanen, M. 2017. Rikollisuustilanne 2016. Rikollisuuskehitys tilastojen ja tutkimusten valossa. Teoksessa Kivivuori, J., Niemi, H., Aaltonen, M., Danielsson, P., Lehti, M., Suonpää, K., Kääriäinen, J., Lappi-Seppälä, T. & Virtanen, M. Katsauksia 22/2017. Helsinki: Helsingin yliopisto. Viitattu 20.2.2024-15.5.2024. https://helda.helsinki.fi/server/api/core/bitstreams/b3d5d9c6-8c05-4aa1-97a1-c19e9aa3b9a3/content

OECD 2006. Identity Fraud: Tax Evasion and Money Laundering Vulnerabilities. Viitattu 15.5.2024. https://www.oecd.org/ctp/crime/identity-fraud-tax-evasion-and-money-laundering-vulnerabilities.htm

Poliisi 2024a. Viitattu 20.2.2024-3.3.2024. https://poliisi.fi/petosrikokset

Poliisi 2024b. Viitattu 3.3.2024. https://poliisi.fi/tietomurrot

Poliisi 2024c. Viitattu 5.3.2024. https://poliisi.fi/kyberrikokset

Poliisi 2024d. Viitattu 5.5.2024. https://poliisi.fi/rahanpesu

Rahanpesun selvittelykeskus. 2023. Rahanpesun selvittelykeskuksen vuosikertomus 2023. Viitattu 5.5.-15.5.2024. https://poliisi.fi/katsauksia-ja-raportteja-rahanpesun-ja-terrorismin-rahoituksen-torjunnasta

Salomaa, L. 2019. Rahanpesurikokset oikeuskäytännössä X – Törkeät rahanpesutuomiot käräjäoikeuksissa 2017 ja 2018. Keskusrikospoliisi. Viitattu 15.4.2024. https://poliisi.fi/documents/25235045/67733116/Rahanpesurikokset-oikeusk%C3%A4yt%C3%A4nn%C3%B6ss%C3%A4-2017-2018+-+T%C3%B6rke%C3%A4t+rahanpesutuomiot+k%C3%A4r%C3%A4j%C3%A4oikeuksissa+2017+ja+2018.pdf/37927f4a-53b9-7574-ef21-e81e86cff9fb/Rahanpesurikokset-oikeusk%C3%A4yt%C3%A4nn%C3%B6ss%C3%A4-2017-2018+-+T%C3%B6rke%C3%A4t+rahanpesutuomiot+k%C3%A4r%C3%A4j%C3%A4oikeuksissa+2017+ja+2018.pdf?t=1632126684820

Savona, E. & Manzoni, F. 2013. European Money Trails. New York: Routledge.

Sisäministeriön sisäisen turvallisuuden sivusto TUOVI 2023. https://sisainenturvallisuus.fi/rikollisuus

Tanttari, S. & Alanko, M. 2017. Petosrikollisuus ja sen ehkäisy - Rikoksentorjuntakatsaus 2017. Oikeusministeriön julkaisu 58/2017. Oikeusministeriö. Viitattu 1.5.–15.2024. http://urn.fi/URN:ISBN:978-952-259-659-8

TEPA-termipankki 2024. Viitattu 11.4.2024. https://termipankki.fi/tepa/fi/haku/ip%20osoite

TEPA-termipankki 2016. Viitattu 4.3.2024. https://termipankki.fi/tepa/fi/haku/valastelu

Verohallinto 2024. Viitattu 5.5.2024. https://www.vero.fi/tietoa-verohallinnosta/verohallinnon_esittely/toiminta/vastuullisuus/verovaj/veroparatiisi/

YLE 2020. Oletko saanut ilmoituksen paketista, jota et tiennyt tilanneesi? Niin tuhannet muutkin, sillä nyt on tekstiviestihuijausten sesonki. Viitattu 4.3.2024. https://yle.fi/a/3-11679223

Wall Street Journal 2023. Digital payment apps offer perks, convenience and security risks. Viitattu 29.4.2024. https://www.wsj.com/podcasts/google-news-update/digital-payment-apps-offer-perks-convenience-and-security-risks/ffa66bcb-dcdc-4197-819e-d3a78abc7f96

Wall Street Journal 2001. Man caught using alias from `The three stooges'. Viitattu 15.5.2024. https://www.proquest.com/newspapers/man-caught-using-alias-three-stooges/docview/398819489/se-2

Oikeuskäytäntö

Korkein oikeus:

KKO:2020:98, 18.12.2020/1978

KKO:2019:110, 19.12.2019/2187

KKO:2009:59, 3.7.2009/1518

Kuviot

Taulukot

Taulukko 6: OECD 2006. Toimintamalleja veronkierron tai rahanpesun järjestämiseksi hyödyntäen varastettua tai väärennettyä henkilöllisyyttä. Viitattu 15.5.2024. https://www.oecd.org/ctp/crime/identity-fraud-tax-evasion-and-money-laundering-vulnerabilities.htm